CA ACF2 r16
Security Target

ST Version: 1.0
June 23, 2017

ca technologies

3333 Warrenville Road
Suite 800
Lisle, IL 60532

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

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

Table of Contents

Table of Figures

Table 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.

1.1.1 ST Identification

ST Title:	CA ACF2 r16 Security Target
ST Version:	1.0
ST Publication Date:	June 23, 2017
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

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

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

Chapter 3 describes the conformance claims made by this ST.

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

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

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

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

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

1.1.3 Terminology

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

Term	Definition
Administrator	Individuals interacting with ACF2 in a capacity where they are attempting to view or modify the functions or security attributes of ACF2 or of other administrators or users.
Command Propagation Facility	A mechanism by which commands issued on one mainframe system are simultaneously transmitted to other systems.
Database	In the context of ACF2, a database is one of three that collectively comprise the Security Database: Infostorage, Logonid, or Rule. Stored as a VSAM file.
Dataset	A filesystem object residing on the mainframe system
Direct Access Storage Device	Any semi-permanent storage mechanism such as a hard disk, magnetic, or optical storage.
Initial Program Load	Synonymous with system startup for z/OS systems.
Interactive System Productivity Facility	A mechanism for abstracting CLI commands behind a more user-friendly menu-driven interface.
Logonid	The username used by an administrator, user, or started task to access the mainframe system
Logonid Record	A record maintained by ACF2 that contains authorization and diagnostic data for an administrator or user. Includes the logonid field.
LPAR	Short for logical partition. One mainframe system can be running multiple instances of z/OS in separate LPARs. Used for redundancy or parallel processing.
Object	Programs, files, configuration settings, and authentication capabilities that exist on z/OS and can be protected by the TOE’s access control policy.
Resource	General term for items or functions on the mainframe system other than datasets. Includes but is not limited to TSO accounts, TSO procedures, commands, programs, transactions, and storage areas.
Role	An administrative grouping that gives all members the same authorizations. An

	administrator can simultaneously belong to multiple roles.
RSRCVLD	An attribute that can be applied to a resource that supersedes the authorizations of a user that is assigned global read/write access privileges.
Ruleset	A collection of individual rules.
RULEVLD	An attribute that can be applied to a dataset that supersedes the authorizations of a user that is assigned global read/write access privileges.
SAFDEF	A type of record that ACF2 uses to automatically process specific SAF calls made to z/OS without additional rule processing.
Started Task	An address space that runs unattended following execution of a START command, analogous to a UNIX daemon.
Subject	A user or a program operating on behalf of a user.
SYSID	A unique identifier for a mainframe system in each environment.
SYSLOG	z/OS system log.
System Authorization Facility	An internal interface that is provided as part of IBM z/OS that is used to identify when system activity is taking place so that this activity can be routed to a security product (such as ACF2) for adjudication.
System Management Facility	A standardized audit log format developed by IBM that is used to present log data from various mainframe applications in a uniform manner.
Time Sharing Option	An application provided by a mainframe system that allows for Unix-like command-line interaction with the system.
UID	Also known as Expanded UID. Contains a user or administrator's logonid as well as organizationally defined attributes (such as department or geographic region). Can serve as identifying information as a subject rather than the logonid in cases where more granular access control rules are desired.
User	Individuals interacting with ACF2 in a capacity where they are attempting to interact with mainframe resources and ACF2 is adjudicating their actions against its access control policy.
Virtual Telecommunications Access Method	A subsystem provided by z/OS to facilitate networking. Used to provide a common interface for applications that are used to access a mainframe remotely.

Volume	A logical identifier used in z/OS for a specific area of physical storage. Analogous to Windows drive letters.
Virtual Storage Access Method	A specific method of file I/O provided by z/OS. Can also refer generically to a file that uses VSAM.

Table 1-1: Product Specific Terminology

1.1.4 Acronyms

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

Acronym	Definition
AC	Access Control
AES	Advanced Encryption Standard
CICS	Customer Information Control System
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CPF	Command Propagation Facility
DASD	Direct Access Storage Device
DSN	Dataset Name
ESM	Enterprise Security Management (note that the acronym 'ESM' also commonly refers to External Security Manager in the context of mainframe security products such as ACF2)
GSO	Global System Option
ICSF	Integrated Cryptographic Services Facility
IPL	Initial Program Load
ISPF	Interactive System Productivity Facility
JCL	Job Control Language
JES	Job Entry Subsystem
LDAP	Lightweight Directory Access Protocol
LPAR	Logical Partition
NDT	Node Descriptor Table
OS	Operating System
OSP	Organizational Security Policy
PM	Policy Management
PP	Protection Profile
SAF	System Authorization Facility
SFP	Security Functional Policy
SMF	System Management Facility
SSH	Secure Shell
STC	Started Task
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSO	Time Sharing Option
VOL	Volume

VSAM	Virtual Storage Access Method
VTAM	Virtual Terminal Access Method

Table 1-2: Acronym Definition

1.1.5 References

As of r16 all product guidance for ACF2 can be found at https://docops.ca.com/ca-acf2-for-z-os/16-0/en. This ST also references the following Common Criteria documentation:

[1] or [AC] Standard Protection Profile for Enterprise Security Management Access Control, version 2.1 (AC PP)

[2] or [PM] Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1 (PM PP)

[3] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001

[4] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002

[5] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003

[6] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004

1.2 TOE Reference

The TOE is CA ACF2 r16.

1.3 TOE Overview

CA ACF2 (also referred to as the TOE) is an Enterprise Security Management product that provides host-based access control to z/OS systems that reside in its Operational Environment. The TOE enforces administrator-configurable rules that control access to mainframe systems and their data, ensuring that resources are protected from unauthorized access. The TOE includes a policy management function that is used to configure a uniform set of access control policies against multiple distinct physical or logical mainframe instances deployed in the enterprise. This is done using the command propagation facility (CPF) method of administration.

The following figure depicts the TOE boundary, with TOE components in grey/blue and Operational Environment components in orange:

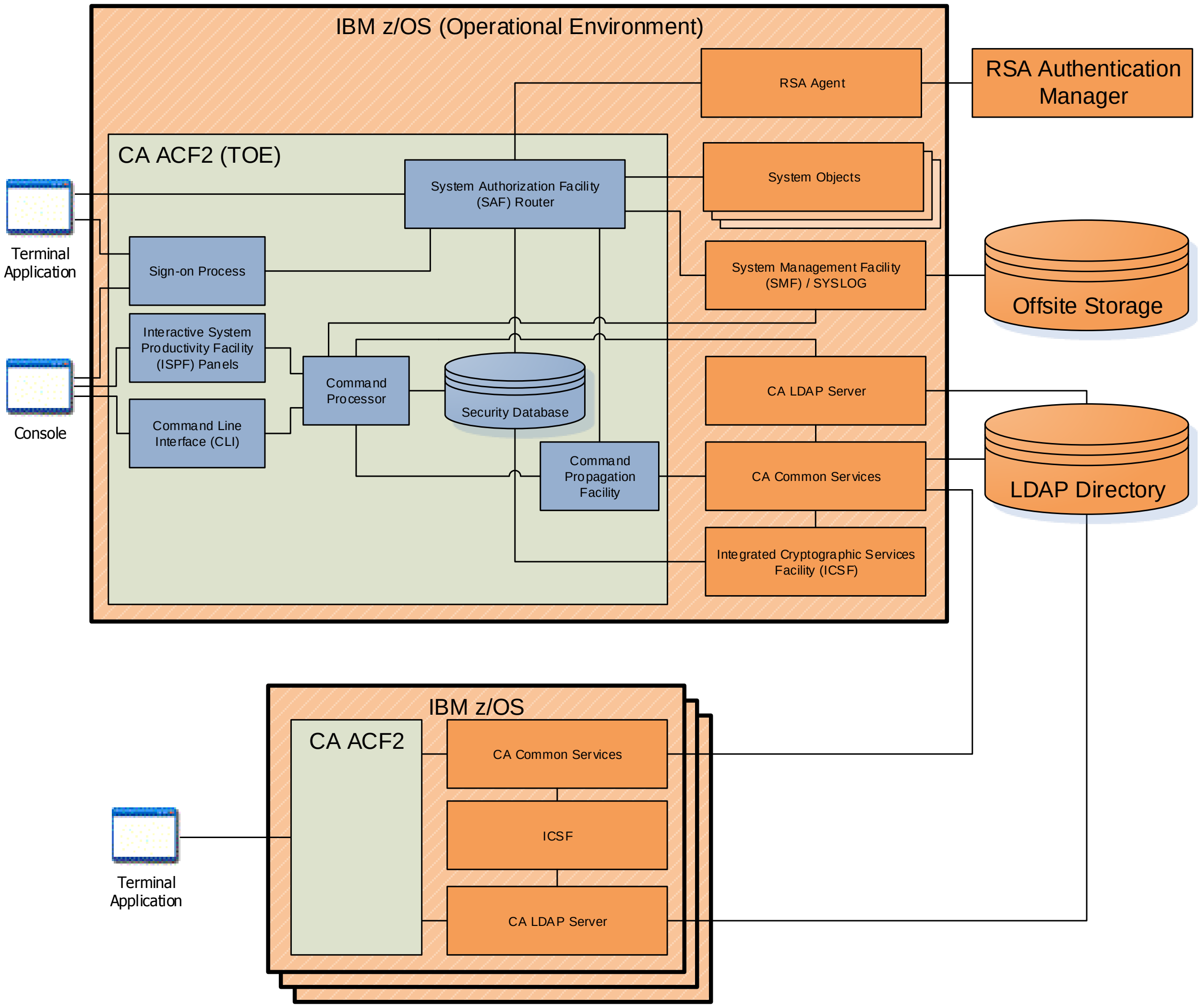
IBM z/OS (Operational Environment)
RSA Agent
RSA Authentication Manager
CA ACF2 (TOE)
System Authorization Facility (SAF) Router
System Objects
Terminal Application
Sign-on Process
System Management Facility (SMF) / SYSLOG
Offsite Storage
Interactive System Productivity Facility (ISPF) Panels
Command Processor
Security Database
CA LDAP Server
Console
Command Line Interface (CLI)
Command Propagation Facility
CA Common Services
LDAP Directory
Integrated Cryptographic Services Facility (ICSF)
IBM z/OS
CA ACF2
CA Common Services
ICSF
CA LDAP Server
Terminal Application

Figure 1-1: TOE Boundary

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

As illustrated in Figure 1-1, CA ACF2 is the lone component of the evaluation. CA ACF2 contains several components within the TOE boundary that are synonymous with CA ACF2 as a product. These components provide the ability to enforce access control policies against resources on the z/OS systems that are part of the Operational Environment as well as the ability for administrators to configure these policies. Because the TOE intercepts all commands issued on the mainframe system, both normal system operation and the administrative usage of CA ACF2 are protected by the TOE's policy enforcement mechanism.

The TOE boundary includes the sign-on process, which performs validation of logon credentials and determines if logon requests are authorized based on access control policy. However, the actual interface where a user or administrator will supply their credentials is not considered to be part of the TOE because this will be through an application that provides an interface to z/OS, such as TSO. Therefore, it is the responsibility of the operational environment to display a warning banner since ACF2 does not present an external interface to a human user that is exclusively for its own use. Any attempt to authenticate to the mainframe system will be directed internally by the OS to the ACF2 sign-on process for evaluation by the TSF.

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

Policy data and user data are stored in the security database which is installed as part of the TOE. To maintain synchronization between distributed systems, user identities are defined in a central LDAP directory in the Operational Environment and are propagated to the TOE via CA LDAP Server, which is a separately installed environmental component running on the mainframe system. CA ACF2 does not have any mechanism to perform active synchronization or reconciliation between the users defined in the security database and in an environmental LDAP server. This sort of functionality is typically expected by an environmental Identity and Credential Management product. The Operational Environment only provides an LDAP interface to the TOE so that remotely-initiated operations against the logonid records defined on the mainframe is possible. The TSF does not exercise any independent control over when this interface is executed, nor does it initiate any outbound communications on its own. The TOE also has the ability to support RSA SecurID token authentication when configured to do so. This requires an administrative mapping between logonid records and RSA SecurID token identities to be performed. Once configured, the TOE will interface with the RSA Agent that resides on the underlying z/OS platform to perform the token authentication.

The TOE records its audit data to the SMF and SYSLOG facilities that are part of the underlying operating system. These are the log facilities that are used by z/OS and other various applications running on it; there is no separate log data stream that is exclusively used by ACF2. As part of general mainframe administration best practices, administrators are expected to back up SMF and SYSLOG data to centralized cold storage on a periodic basis. An organization that does this will also ensure that ACF2 log data generated on all the various CPF nodes will be aggregated in a central location so that audit review of activities performed throughout the environment can be performed from a single point.

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

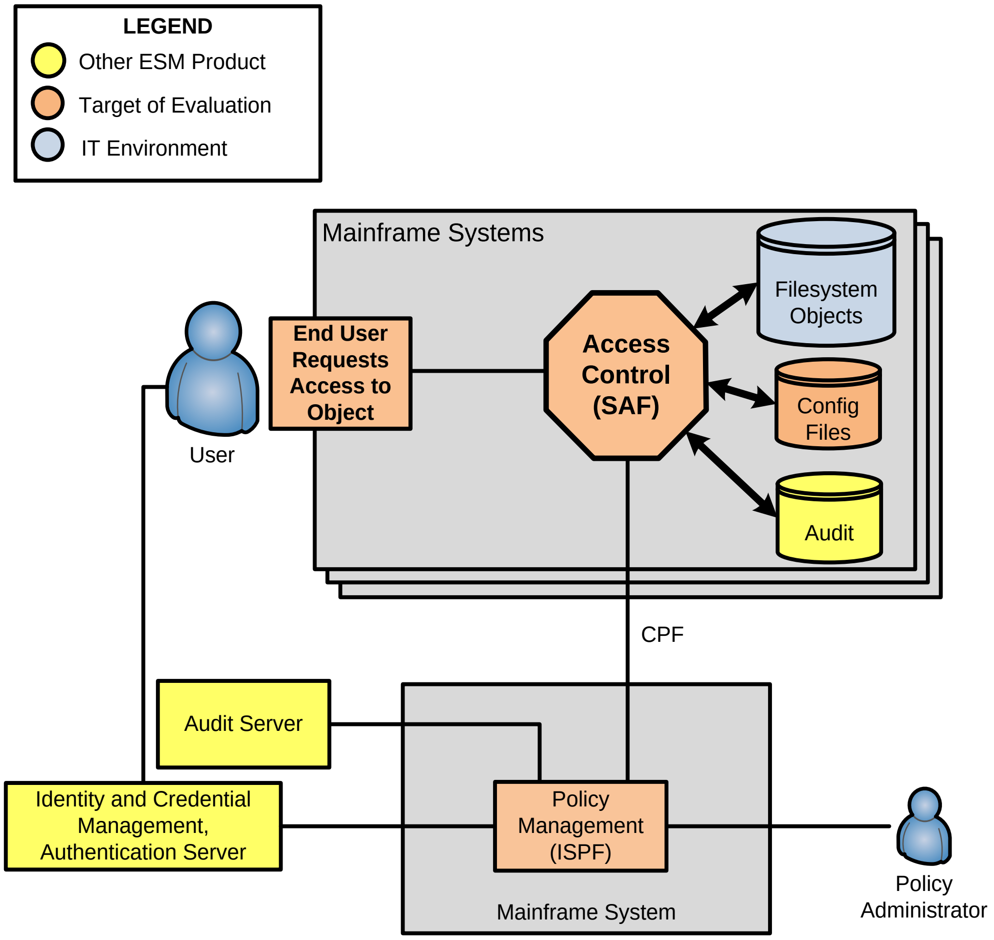

Figure 1-2: ESM PP context for the TOE

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

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

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

1.4 TOE Type

The TOE type for ACF2 is Enterprise Security Management, specifically Host-Based Access Control and Policy Management. The TOE includes an agent that runs on a mainframe system to provide access control to resources on the mainframe system as well as the capability to administer this agent. Using CPF, management commands issued on one instance of the TOE can be transmitted through the Operational Environment to other systems, allowing for simultaneous administration of multiple systems.

2 TOE Description

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

2.1 Evaluated Components of the TOE

The TOE is limited to CA ACF2, which at a general level provides both the means to enforce access controls against protected system resources, the interface to define these rules, and the repository in which rule information is stored. The following table describes the TOE components in the evaluated configuration:

Component	Definition
Command Line Interface (CLI)	The CLI provides a mechanism to configure the TOE.
Command Processor	A TOE subsystem that is responsible for receiving administrative commands from different external interfaces and parsing them into a standardized format that the TSF will interpret.
Command Propagation Facility (CPF)	The CPF provides a single-point management capability that allows CA ACF2 commands issued on one system to be propagated to distributed systems or to different logical partitions (LPARs) of the same system.
Interactive System Productivity Facility (ISPF) Panels	The ISPF interface provides a standardized menu-driven management interface for the issuance of ACF2 commands. The management activities that can be performed using ISPF panels are equivalent to those that can be performed using the CLI.
Security Database	The ACF2 Security Database includes the Logon ID database, the rules database, and the info-storage database. Together these databases are used to define the access control policy that is applied to the z/OS system as well as the subject attributes that are used to govern access requests.
Sign-on Process	The sign-on process intercepts authentication requests made to the mainframe system which allows the TSF to determine whether the requests are valid.
System Authorization Facility (SAF) Router	The IBM System Authorization Facility (SAF) provides a system-wide interface to CA ACF2. The key component that SAF uses is the CA SAF Router (a component of CA ACF2). All RACROUTE and UNIX System Services 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 the unique processing needed to provide full security coverage for the z/OS platform.

Table 2-1: Evaluated Components of the TOE

2.2 Components and Applications in the Operational Environment

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

Component	Definition
CA LDAP Server	In the Operational Environment, an LDAP directory is used to provide a centralized definition for user identities. CA LDAP Server is a z/OS application that is used to translate LDAP communications from an LDAP directory into commands that will synchronize the TOE's users with those defined in LDAP.
Chorus Software Manager (CSM)	CA Chorus Software Manager is a utility that simplifies the acquisition and maintenance of mainframe software. In the evaluated configuration, CSM will be used to install the TOE.
Common Services	CA Common Services is a set of common components used by several CA's mainframe products. It supports the TOE specifically by providing TCP/IP communications services that are used to support remote communications. Common Services delivers the CPF functionality mentioned in Table 2-1
Integrated Cryptographic Services Facility (ICSF)	IBM ICSF is the default cryptographic engine provided by z/OS. It supports the TOE by providing services that allow for remote TCP/IP communications to be encrypted. **Note that ICSF is responsible for generation of cryptographic keys used in trusted communications. As per the FIPS 140-2 Security Policy for ICSF (CMVP certificate #2763), the vendor assumes that a minimum of 384 bits of entropy is used to seed the DRBG to perform this function.**
RSA Agent	A z/OS application that brokers authentication attempts that use RSA SecurID token authentication.
RSA Authentication Manager	A service that resides within the organization that maintains a repository of RSA SecurID tokens and can determine if authentication attempts using RSA SecurID are valid.
SYSLOG	The z/OS system log (SYSLOG) is a collection of SPOOL data that contains console messages, operator commands, and operator responses for the OS. Data regarding administrative use of the TOE will be recorded to SYSLOG automatically as part of the behavior of the console.
System Management Facility (SMF)	SMF is a component of IBM z/OS that provides a standardized logging format for z/OS programs. The TOE's audit data is transmitted to the Operational Environment as SMF logs.

Terminal	The terminal is a remote interface used to administer the TOE or operate the mainframe system. A mainframe operator will use a TN3270e class terminal emulator to interact and interface with the mainframe.
z/OS	IBM z/OS is the mainframe operating system on which CA ACF2 is installed. The TOE has been tested on z/OS version 2.1 with the IBM SSL Cryptographic Module (CMVP certificate #2829) and IBM ICSF PKCS#11 Cryptographic Module (CMVP certificate #2763).

Table 2-2: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

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

2.3.1 Not Installed

These components are not installed with CA ACF2 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.
- **Compliance Event Manager Integration** – Compliance Event Manager allows Administrators to collect, and report on security relevant activity, and generate alerts requiring action when possible compliance violations occur. It has no security impact on the TOE and is not included in the evaluated configuration of the TOE.
- **CA ACF2 Option for DB2 UDB** – CA ACF2 Option for DB2 UDB is outside the scope of the evaluated configuration because it is used to provide fine-grained access controls to database environments. In the evaluated configuration, the scope of the TOE is limited to the access control functionality that mandated by the AC PP for host-based access control, which does not include databases.
- **DFSMS** – DFSMS is an IBM designation for the DF/HSM, DFDSS, DFSORT, DFRMM, and RACF products when used in a DFSMS system. It is not a necessary component for CA ACF2 because the TOE contains its own databases to perform the same functionality.

By default, none of these components are implemented by ACF2. Therefore, administrators do not need to take any specific actions to prevent their use.

2.3.2 Installed but Requires a Separate License

No components are installed that require a separate license.

2.3.3 Installed but Not Part of the TSF

These components are installed with CA ACF2 but are not included in the TSF.

- **Group Logon Parameter** – CA ACF2 only validates the use of the GROUP logon parameter if the user specifies a group that is not the default specified in his logonid record. This functionality is not commonly used for the current functions of the product and is only supported for backward compatibility. The functionality provided by this is not used for object access by the TOE.
- **UADS or No UADS (User Attribute Data Set)** – An obsolete feature that is not part of the evaluated configuration. The advantages of bypassing UADS are faster logon processing and eliminating the need to maintain both UADS and the 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. In the evaluated configuration, CPF will be used for administration of distributed systems.
- **Non-Abort Mode of operation** – ACF2 provides a configurable security mode option that affects the global enforcement of access control policy rules. When the product is first installed, the default setting for this mode is Quiet, which means the product acts as if it is not even present on the system. As part of a typical rollout process, administrators will typically escalate the security mode over a period once they are certain the access control rules that are being put in place will not adversely affect the behavior of the mainframe system. The TOE is not considered to be in its evaluated configuration until it has been set into Abort mode, which is the only mode that will block access attempts that are not permitted by policy.

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

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

2.4 Physical Boundary

The physical boundary of the TOE includes the CA ACF2 software that is installed on the mainframe system. The TOE does not include the hardware or operating systems of the systems on which it is installed. It also does not include the third-party software which is required for the TOE to run. The following table lists the minimum system requirements needed to use the TOE:

Component	Requirement

Platform	IBM System z mainframe (zEC12, z114, z196, z9 series, z10 series, z13)
Disk Storage	700 MB or greater
Operating System	IBM z/OS, version 2.1 RSU1506 (Recommended Service Upgrade) or higher
System Components	• INIT/JOB • JES2 • TSO • TCP/IP • VTAM • CA Common Services for z/OS r14.1 or above • CA LDAP Server for z/OS r15.1
Cryptographic Capabilities	• IBM ICSF • IBM System SSL • IBM Ported Tools for z/OS - OpenSSH

Table 2-3: Operational Environment System Requirements

2.5 Logical Boundary

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

1. Enterprise Security Management
2. Security Audit
3. Communications
4. User Data Protection
5. Identification and Authentication
6. Security Management
7. Protection of the TSF
8. Resource Utilization
9. TOE Access
10. Trusted Path/Channels

2.5.1 Enterprise Security Management

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

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

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

2.5.2 Security Audit

The TOE generates SMF records of all its functions, including enforcement of access control rules and execution of configuration changes. The SMF records are protected by the TSF but this facility itself is a native z/OS component and part of the Operational Environment. An administrator can configure the types of events for which logs are generated.

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

2.5.3 Communications

The TOE provides feedback to administrators when changes to policy rules are attempted. The TOE returns the SYSID of the target system along with the success or failure of the attempted change. The CPF journal file maintained by ACF2 records the CPF activities performed and their results.

2.5.4 User Data Protection

The TOE performs host-based access control against mainframe systems. Access control policies can protect processes, files, system configuration, and use of the authentication function from various actions on z/OS systems. Policies can be applied to users on endpoint systems as well as started tasks that interact with system resources. Users can be identified either individually through their logonid or collectively based on common values in the expanded UID of multiple users. The TSF controls access based on subject identity based on subjects that are defined internally to the mainframe. Subject data is encapsulated as a logonid record, which the TSF maintains and uses to make access control decisions. The access that is allowed to users is based on rules. When no rule is present for a requested action, access is denied.

The TSF can associate subjects and objects with certain attributes that will bypass the rule validation process to automatically have the request be allowed or denied, depending on the attributes. In the evaluated configuration, the only bypasses that have been claimed are SAFDEF and the SECURITY, READALL, and NON-CNCL logonid attributes.

Since the TSF operates in a deny-by-default posture, objects that comprise the TOE on the local system are protected from unauthorized modification.

2.5.5 Identification and Authentication

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

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

2.5.6 Security Management

By default, the TOE defines several administrative roles that determine the options available to users who are assigned to these roles. The TOE also can define scope records so that users can only perform administrative actions against certain subsets of subjects or objects on the system. A Policy Administrator as defined by the PM PP is any administrator with sufficient privileges to manage some aspect of the TSF. The TOE operates in a deny-by-default posture so the enforced access control policy is restrictive by default. Administrators use ISPF panels or individual commands to manage the policy enforced by the TOE as well as users and auditable events.

The Node Descriptor Table (NDT) defines authorized and active senders and receivers of CPF commands, so remote management can only be initiated by authorized and compatible instances of ACF2. Distributed components trust one another by shared certificates that are managed by Common Services.

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

The TOE's policy engine prevents the definition of ambiguous policies by defining a strict order of precedence for which rules are enforced first. For example, deny rules always take precedence over allow rules for the same subject and rules that apply to a specific subject always take precedence over rules that apply to a group that the subject belongs to. In cases where two rules are identical in every respect except for the permissions associated with the rule, the TSF will prevent the ruleset from being compiled until the conflict is resolved.

2.5.7 Protection of the TSF

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

If an error occurs that causes the TOE to be shut down, any security checks that would have been made will require manual intervention from a console operator to approve. The TOE will also automatically attempt to restart itself in this situation.

Systems receiving management commands remotely via CPF will protect themselves from replayed policy data through obfuscation of the contents of the remote command, token authorization information being passed in the header of the command, and remote TCP/IP communications being secured using TLS. Replay attempts will be rejected as invalid or unauthorized commands.

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

2.5.8 Resource Utilization

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

2.5.9 TOE Access

The TOE's access control policy enforcement engine can control access to the mainframe system's authentication function based on date, time, and/or source of the attempt. LDAP is only used to define identity data that is then synchronized with the TOE's internal database and is not used for authentication; the TSF is in full control of the authentication function.

2.5.10 Trusted Path/Channels

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

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

3 Conformance Claims

3.1 CC Version

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

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) are conformant to Part 2 extended to include all applicable NIAP and International interpretations through June 23, 2017.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) are conformant to Part 3 to include all applicable NIAP and International interpretations through June 23, 2017.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profiles:

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

3.5 Package Claims

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

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

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

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

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

3.6 Package Name Conformant or Package Name Augmented

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

3.7 Conformance Claim Rationale

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

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

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

4 Security Problem Definition

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

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

4.1 Threats

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

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

Table 4-1: Threats

4.2 Organizational Security Policies

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

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

Table 4-2: TOE Organizational Security Policies

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

4.3 Assumptions

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

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

4.3.1 Personnel Assumptions

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

Table 4-3: Personnel Assumptions

4.3.2 Physical Assumptions

No physical assumptions have been defined for the TOE.

4.3.3 Connectivity Assumptions

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

Table 4-4: Connectivity Assumptions

4.4 Security Objectives

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

4.4.1 TOE Security Objectives

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

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

Table 4-5: TOE Objectives

Note the following in the above table:

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

4.4.2 Security Objectives for the Operational Environment

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

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

Table 4-6: TOE Operational Environment Objectives

Note the following in the above table:

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

4.4.3 Operational Environment Components Rationale

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

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

Table 4-7: Operational Environment Components Rationale

4.5 Security Problem Definition Rationale

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

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

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

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

5 Extended Components Definition

5.1 Extended Security Functional Requirements

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

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

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

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

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

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

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

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

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

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

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

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class ESM: Enterprise Security Management

6.3.1.1 [PM]ESM_ACD.1 Access Control Policy Definition

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

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

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

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

6.3.1.2 [PM]ESM_ACT.1 Access Control Policy Transmission

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

6.3.1.3 [PM]ESM_ATD.2 Subject Attribute Definition

[PM]ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: [

- **logonid record (containing logonid, expanded UID, cancel flag, suspend flag, trace flag, violation count, privileges),**
- **privilege attributes (NON-CNCL, READALL, SECURITY, TSO),**
- **role (group) membership**].

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

6.3.1.4 [PM]ESM_EAU.2 Reliance on Enterprise Authentication

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

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

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

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

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

6.3.2 Class FAU: Security Audit

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

[AC+PM]FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

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

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

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

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

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

Table 6-2: Auditable Events

[AC+PM]FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**the information in Table 6-2**].

6.3.2.2 [AC]FAU_SEL.1 Selective Audit

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

a) [subject identity]; and

b) [**rule triggered, authorization result**]

6.3.2.3 [PM]FAU_SEL_EXT.1 External Selective Audit

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

a) [subject identity]; and

b) [**rule triggered, authorization result**]

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

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

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

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

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

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

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

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

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

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

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

6.3.3 Class FCO: Communications

6.3.3.1 [AC]FCO_NRR.2 Enforced Proof of Receipt

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

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

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

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

6.3.4 Class FDP: User Data Protection

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

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

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

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

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

- subjects: subset of users from an organizational data store, [**no additional subjects**]; and
- objects: programs, files, and configuration values that comprise or contain TOE data, [**no additional objects**];

and

- operations: ability to create, read, modify, execute, delete, terminate, or change permissions of objects, [**no additional operations**]

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

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

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

Table 6-3: Access Control SFP

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

- **If no rule exists to govern access to an object, access to that object is denied by default.**
- **The object must be accessed during a date or time that is authorized by the applicable rule(s).**
- **The object must be accessed from a source and using an application that is authorized by the applicable rule(s).**
- **Masking values can be used to have rules apply simultaneously to multiple subjects and/or objects.**
- **Subjects are identified by their username, UID, or any group memberships that they have.**
- **The requested access type (read, write, allocate, execute) must be authorized.**
- **Conflicting rules take precedence over one another**

based on applicability].

Application Note: *Hierarchy of rule applicability is defined in the TSS.*

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

- **SAFDEF can be used to bypass security checking and automatically return a predetermined result.**
- **SECURITY user attribute will grant bypass of all access control rules for read and write operations unless the target object has the RULEVLD or RSRCVLD attribute.**
- **READALL user attribute will grant bypass of all access control rules for read operations unless the target object has the RULEVLD or RSRCVLD attribute.**
- **NON-CNCL user attribute will grant bypass of all access control rules for read and write operations without exception.**
- **Program objects cannot be accessed unless the subject has NON-CNCL and/or SECURITY attributes**
- **By default, a user can access objects they own even if no rule exists to grant access**].

[AC]FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

- **SAFDEF can be used to bypass security checking and automatically return a predetermined result.**
- **If rule associates a dataset or resource object with the RULEVLD or RSRCVLD attribute, it cannot be bypassed by a user with the SECURITY or READALL attribute**].

Application Note: *SAFDEF can be either a positive or negative bypass of rule checking, depending on administrator configuration of the SAFDEF.*

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

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

[AC]FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: the TOE will not permit requested operations against objects that are defined to be protected unless the acting subject is the individual that was responsible for the TOE’s installation and initial configuration.

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

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

6.3.5 Class FIA: Identification and Authentication

6.3.5.1 [PM]FIA_AFL.1 Authentication Failure Handling

[PM]FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [**1-32,767**]] unsuccessful authentication attempts occur related to [**authentication to the mainframe system**].

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

6.3.5.2 [PM]FIA_USB.1 User-Subject Binding

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

[PM]FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**a user's logonid record is associated with the user at initial authentication to the system. Security-relevant security attributes that pertain to administrators are their logonid and their management roles as defined by FMT_SMR.1. Scope records are associated with a user's logonid**].

Application Note: *If a field is not applicable to a user, it is omitted from the logonid record.*

The logonid record contains security attributes as well as diagnostic data about the user's access history.

Expanded UID data can include organizationally-defined fields.

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

6.3.6 Class FMT: Security Management

6.3.6.1 [PM]FMT_MOF.1 Management of Functions Behavior

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

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

Table 6-4: Management Functions by Role

Application Note: SECURITY is used to denote that administrators with the*

ACCOUNT role can only modify administrators with the SECURITY role if they themselves also have the SECURITY role.

Users with the AUDIT role can determine the behavior of all listed functions but cannot modify their behavior.

All of the permissions listed above are the default permissions defined in the ACF Field Definition Record (ACFFDR). Modification of the ACFFDR or application of scope rules can affect the permissions of individual administrators or all members of a particular administrative role.

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

[AC]FMT_MOF.1.1(1)	The TSF shall restrict the ability to [determine the behavior of, modify the behavior of] the functions[: audited events, repository for remote audit storage, Access Control SFP, policy being implemented by the TSF, Access Control SFP behavior to enforce in the event of communications outage, [**no other functions**]] to [an authorized and compatible Policy Management product].
Application Note:	*The TSF automatically enforces secure behavior for repository for remote audit storage and for Access Control SFP behavior to enforce in the event of communications outage so these functions are not configurable.* *This SFR was written from the perspective of an Access Control product being a standalone TOE. For CA ACF2, "the TSF" and "an authorized and compatible Policy Management product" should both be interpreted as "CA ACF2".*

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

[AC]FMT_MOF.1.1(2)	The TSF shall restrict the ability to [determine the behavior of] the functions[: policy being implemented by the TSF, [**no other functions**]] to [an authorized and compatible Policy Management product].
Application Note:	*This SFR was written from the perspective of an Access Control product being a standalone TOE. For CA ACF2, "the TSF" and "an authorized and compatible Policy Management product" should both be interpreted as "CA ACF2".*

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

[PM]FMT_MOF_EXT.1.1	The TSF shall restrict the ability to query the behavior of, modify the behavior of the functions of Access Control products: audited events, repository for remote audit storage, Access Control SFP, policy being implemented by the TSF, Access Control SFP behavior to enforce in the event of communications outage, [**no other functions**] to [**administrators who belong to the SECURITY role and have appropriate scope**].
Application Note:	*The TSF automatically enforces secure behavior for repository for*

remote audit storage and for Access Control SFP behavior to enforce in the event of communications outage so these functions are not configurable.

This SFR was written from the perspective of a Policy Management product being a standalone TOE. For CA ACF2, "the TSF" and "Access Control products" should both be interpreted as "CA ACF2".

6.3.6.5 [AC]FMT_MSA.1 Management of Security Attributes

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

Application Note: *This SFR was written from the perspective of an Access Control product being a standalone TOE. For CA ACF2, "the TSF" and "an authorized and compatible Policy Management product" should both be interpreted as "CA ACF2".*

6.3.6.6 [AC]FMT_MSA.3 Static Attribute Initialization

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

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

Application Note: *This SFR was written from the perspective of an Access Control product being a standalone TOE. For CA ACF2, "the TSF" and "an authorized and compatible Policy Management product" should both be interpreted as "CA ACF2".*

6.3.6.7 [PM]FMT_MSA_EXT.5 Consistent Security Attributes

[PM]FMT_MSA_EXT.5.1 The TSF shall [identify the following internal inconsistencies within a policy prior to distribution: [**rules with identical subjects, objects, and operations but differing authorizations**]].

[PM]FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: [issue a prompt for an administrator to manually resolve the inconsistency].

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

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

SFR	Management Activity
[PM]ESM_ACD.1	Creation of policies
[PM]ESM_ACT.1	Transmission of policies
[PM]ESM_ATD.2	Association of attributes with subjects
[PM]ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
[AC+PM]ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
[PM]FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
[PM]FAU_STG_EXT.1	Configuration of external audit storage location
[PM]FIA_AFL.1	Configuration of authentication failure threshold value
	Configuration of actions to take when threshold is reached
	Execution of restoration to normal state following threshold action (if applicable)
[PM]FIA_USB.1	Definition of subject security attributes, modification of subject security attributes
[PM]FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
[PM]FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable).
[PM]FMT_SMR.1	Management of the users that belong to a particular role
[PM]FTA_TAB.1	Maintenance of the banner
[AC+PM]FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)
[PM]FTP_TRP.1	Configuration of actions that require trusted path (if applicable)

Table 6-5: TSF Management Functions

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

[AC+PM]FMT_SMR.1.1 The TSF shall maintain the roles [**ACCOUNT, AUDIT, CONSULT, LEADER, SECURITY, USER**].

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

6.3.7 Class FPT: Protection of the TSF

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

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

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

6.3.7.2 [AC]FPT_FLS_EXT.1 Failure of Communications

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

6.3.7.3 [AC]FPT_RPL.1 Replay Detection

[AC]FPT_RPL.1.1 The TSF shall detect replay for the following entities: [**entities which use replay to impersonate CPF commands issued by the TOE**].

[AC]FPT_RPL.1.2 The TSF shall perform [**the following action: reject the replayed policy**] when replay is detected.

6.3.7.4 [AC+PM]FPT_SKP_EXT.1 Protection of Secret Key Parameters

[AC+PM]FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.3.8 Class FRU: Resource Utilization

6.3.8.1 [AC]FRU_FLT.1 Degraded Fault Tolerance

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

6.3.9 Class FTA: TOE Access

6.3.9.1 [AC+PM]FTA_TSE.1 TOE Session Establishment

[AC+PM]FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [day, time, [**APPLID, suspend status**]].

6.3.10 Class FTP: Trusted Path/Channels

6.3.10.1 [AC+PM]FTP_ITC.1 Inter-TSF Trusted Channel

[AC+PM]FTP_ITC.1.1 Refinement: The TSF shall use [TLS] to provide a *trusted* communication channel between itself and *authorized IT entities* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

Application Note: *The TLS protocol implementation is provided by the underlying platform on which the TOE is installed.*

[AC+PM]FTP_ITC.1.2	The TSF shall permit [<u>the TSF</u>**]** to initiate communication via the trusted channel.
[AC+PM]FTP_ITC.1.3	Refinement: The TSF shall initiate communication via the trusted channel for *transfer of policy data*, [**no other functions**].

6.3.10.2 [PM]FTP_TRP.1 Trusted Path

[PM]FTP_TRP.1.1	Refinement: The TSF shall *use* [<u>SSH</u>] *to* provide a *trusted* communication path between itself and remote users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification, disclosure.
Application Note:	*The SSH protocol implementation is provided by the underlying platform on which the TOE is installed.*
[PM]FTP_TRP.1.2	The TSF shall permit [remote users] to initiate communication via the trusted path.
[PM]FTP_TRP.1.3	Refinement: The TSF shall require the use of the trusted path for *initial user authentication, execution of management functions.*

6.4 Statement of Security Functional Requirements Consistency

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

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

7 Security Assurance Requirements

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

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 Developer action elements:

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

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

7.1.1.2 Content and presentation elements:

ADV_FSP.1.1C

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

ADV_FSP.1.2C

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

ADV_FSP.1.3C

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

ADV_FSP.1.4C

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

7.1.1.3 Evaluator action elements:

ADV_ FSP.1.1E

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

ADV_ FSP.1.2E

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

7.2 Class AGD: Guidance Documentation

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 Developer action elements:

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 Content and presentation elements:

AGD_OPE.1.1C

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

AGD_OPE.1.2C

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

AGD_OPE.1.3C

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

AGD_OPE.1.4C

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

AGD_OPE.1.5C

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

AGD_OPE.1.6C

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

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 Evaluator action elements:

AGD_OPE.1.1E

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

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 Developer action elements:

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 Content and presentation elements:

AGD_ PRE.1.1C

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

AGD_ PRE.1.2C

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

7.2.2.3 Evaluator action elements:

AGD_ PRE.1.1E

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

AGD_ PRE.1.2E

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

7.3 Class ALC: Life Cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 Developer action elements:

ALC_CMC.1.1D

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

7.3.1.2 Content and presentation elements:

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 Evaluator action elements:

ALC_CMC.1.1E

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

7.3.2 TOE CM Coverage (ALC_CMS.1)

7.3.2.1 Developer action elements:

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 Content and presentation elements:

ALC_CMS.1.1C

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

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 Evaluator action elements:

ALC_CMS.1.1E

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

7.4 Class ATE: Tests

7.4.1 Independent Testing - Conformance (ATE_IND.1)

7.4.1.1 Developer action elements:

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 Content and presentation elements:

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 Evaluator action elements:

ATE_IND.1.1E

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

ATE_IND.1.2E

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

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 Developer action elements:

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 Content and presentation elements:

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 Evaluator action elements:

AVA_VAN.1.1E

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

AVA_VAN.1.2E

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

AVA_VAN.1.3E

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

8 TOE Summary Specification

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

8.1 Enterprise Security Management

8.1.1 [PM]ESM_ACD.1:

Administrators of ACF2 can define access control policies by using the CLI or ISPF panels within the mainframe system. These policies can be simultaneously transmitted to one or more remote systems using the Command Propagation Facility (CPF) and processed by separate instances of the TOE running on those systems.

CA ACF2 is an integrated product that provides both Policy Management and Access Control capabilities, so there are no compatibility considerations for the ability to define policies. Every single operation that the Access Control component is capable of controlling is something that can be defined in a policy by the Policy Management component. Therefore, the subjects, objects, and operations that the TSF can enforce access control policies against are the same set of subjects, objects, and operations that can be defined in an access control policy. Information about the subjects, objects, and operations that the TSF can control access to is provided in section 8.4.

Each instance of ACF2 only instantiates a single policy at one time. The policy identifier is synonymous with the unique SYSID value of the mainframe or LPAR on which ACF2 is installed. Within a given policy, rules are identified by line number, which is subject to change as rules are added or removed.

8.1.2 [PM]ESM_ACT.1:

When an administrator enters a command that will affect the behavior of ACF2's access control mechanism, the changes are immediately propagated to the local database(s). If ACF2 is being used to administer multiple systems via CPF, the administrative commands are sent to Common Services and transmitted to the other systems. If a remote CPF node is unavailable, the node is periodically checked for availability and the administrative commands are sent once the node is available. Remote TCP/IP communications (as opposed to other partitions on the same local mainframe system) are secured by Common Services using TLS.

8.1.3 [PM]ESM_ATD.2:

ACF2 maintains a logonid record for each user of the mainframe system. A logonid contains the following security-relevant attributes with respect to the claimed Protection Profiles:

- logonid – the username that the user uses to log in to the system.
- expanded UID – an expanded username that can include organizationally-defined data such as department, function, or geographic region. Access rules can be written against expanded UID data to conveniently organize users into groups.
- cancel – an administratively settable flag that forbids the user from accessing the system if set.
- suspend – a temporary flag that will suspend a user's ability to access the system for a set period.

- expire – if the logonid is suspended, the expire field defines the date and time that the suspension will expire.
- trace – a flag that logs all actions performed by the user when set.
- privileges – the administrative roles (e.g. SECURITY, AUDIT) associated with the user.
- violation count – identifies the number of failed logon attempts made by the logonid which is used to determine if the account should be locked out for excessive violations.

The following privilege attributes apply to the user's ability to access resources protected by the TSF:

- NON-CNCL – a user with this privilege has full access to any objects that reside on the TOE. Access attempts that would not typically be allowed by the access rules are logged but the attempts will succeed.
- READALL – like NON-CNCL, but only with read operations.
- SECURITY – a user with this privilege has access to all resources protected by the TSF.
- TSO – a user with TSO privileges on their logonid can access the mainframe using TSO.

Note that the SECURITY and READALL privileges can be overridden by explicit negative overrides as defined in FDP_ACF.1.4(1).

Using CA LDAP Server, the mainframe can receive changes that are made to a centralized LDAP repository in the Operational Environment and convert them to equivalent commands that are recognized by the TOE. This allows for an organization to synchronize user account data with other mainframe environments as well as other systems or applications.

In addition to logonid records, ACF2 maintains a role table for all users. A user's role table is built at system entry similar to the logonid. Roles for users are arbitrary and administrator-defined and can be thought of as groups when writing rules against them.

8.1.4 [PM]ESM_EAU.2:

For administrators to access ACF2, they must be identified and authenticated to the mainframe system on which it is installed. In the evaluated configuration, administrator accounts are defined as users on the mainframe system itself. A user or administrator wishing to access the mainframe will invoke the desired interface (such as TSO) and provide their credentials to it. The authentication request is received by the TOE's sign-on process, which interfaces internally with SAF to determine if the authentication request is valid, both in terms of correct credentials and in terms of whether the TOE's access control policy will grant access to the system based on the logonid making the request, the interface or application they are attempting to use, and the day/time of the request. This is described in more detail under **[AC+PM]**FTA_TSE.1. When the TOE is configured to use RSA SecurID token authentication, a mapping between logonids and SecurID token IDs will be defined within the TSF.

The administrator connects to the mainframe system using a TN3270e terminal emulator and provides their username and password or RSA SecurID token value to the system for validation. If the credentials are valid and the TSF determines that the authentication should be permitted, the administrator is granted access to the mainframe. To determine if an RSA SecurID token value is accurate, the TSF will interface with the environmental RSA Agent based on the RSA SecurID token ID mapped to the logonid requesting access. The RSA Agent will communicate with the central RSA Authentication Manager and return an appropriate response to the TOE. Authentication behavior is not affected by the presence of an LDAP directory in the Operational Environment. Authentication requests will always be handled internally by the mainframe system against the system's own access control policy and logonid database. Any change made to an environmental LDAP directory would also need to be propagated to the TOE's logonid database for it to affect the behavior of the mainframe system. The environmental CA LDAP Server component provides an LDAP interface to the TSF to facilitate this.

8.1.5 [AC+PM]ESM_EID.2:

All users log in to the mainframe system on which ACF2 is installed by providing their username and password that are defined within the mainframe system itself. When a user is first logged in, ACF2 associates the user with their logonid record. This record allows the user to identify itself for access control policy enforcement, either through their username or through an expanded UID. In the case where RSA SecurID token authentication is used, the user will have an RSA SecurID token with a unique ID. This is mapped to the user's logonid within the ACF2 Security Database. When a user attempts to authenticate to the TOE using their SecurID token, the correct token ID will be used when querying the RSA Authentication Manager based on this mapping.

Since ACF2 is itself considered to be a system resource just like every other object on the mainframe that is protected by the TSF, there is no distinction between how users and administrators identify themselves.

8.2 Security Audit

8.2.1 [AC+PM]FAU_GEN.1:

Audit data is generated by ACF2 for both administrative activity and for access attempts made against environmental resources that are mediated by ACF2. The startup and shutdown of ACF2 itself is audited, as is any change to the set of auditable events.

The auditable events for security-relevant activities are defined in Table 6-2. Each audit record contains fields to record date, time, event type, subject identity (if applicable), and outcome information. Some audit records define additional information; the records and information are listed in Table 6-2.

8.2.2 [AC]FAU_SEL.1:

The auditable events that are actually audited by ACF2's access control functionality are dependent on the configuration of the rules that are being enforced. By default, logs will be generated for all access attempts that are rejected by a rule. Rules that are written using the ALLOW parameter will not generate logs when they authorize requests but rules that are written using the LOG parameter will both authorize the request and generate a log. Additionally, logging can be enabled or disabled for individual operations within a rule. For example, the following ruleset allows all users with UIDs that begin with 'AB' to read and write to the dataset PROD.DATASET.NR1. However, any writes made by users whose UIDs begin with 'ABC' will also be logged:

```
$KEY(PROD)

DATASET.NR1 UID(ABC) R(ALLOW) W(LOG)

DATASET.NR1 UID(AB) R(ALLOW) W(ALLOW)
```

Alternatively, if the TRACE attribute is enabled for a user, all activities performed by that user will be logged regardless of how the rules are defined.

8.2.3 [PM]FAU_SEL_EXT.1:

Administrators use ACF2's management interface to configure the set of auditable events by subject through configuration of the subject's logonid record. The auditing for individual rules (or individual operations within a rule) is controlled through the configuration of those rules.

8.2.4 [AC]FAU_STG.1:

Audit data is stored locally on the mainframe system using SMF and SYSLOG. The amount of storage space allocated to these facilities is defined by z/OS and is not controlled by ACF2. SMF and SYSLOG are both the common repositories for audit storage on the mainframe so other mainframe applications may be using these facilities in addition to ACF2. SMF writes to files named SMF.MANx, where "x" typically designates a sequential alphanumeric value. SYSLOG data is typically written to sequential files named SYSLOGxx, beginning with 00. Since these are files that reside on the mainframe system, they are automatically protected by ACF2 and access to them can be granted on a per-rule basis.

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

8.2.5 [AC+PM]FAU_STG_EXT.1:

All audit data that is recorded on the mainframe system, including for ACF2, gets written to SMF or SYSLOG. SMF and SYSLOG are both environmental components that reside on the local z/OS system. These facilities act as generalized audit storage repositories for the OS itself as well as any applications that run on it such as ACF2. ACF2 does not write its audit data to a specialized repository that is exclusively for its own use. Instead, ACF2 writes its audit data to the generalized logging facilities that are provided by the OS. Therefore, any offsite backup/storage of audit data is a function initiated on the z/OS system and is not handled by ACF2. For example, a job can be written to back up the SYSLOG data stored on the JES spool to a permanent storage location on the local OS using the IASXWR00 program to extract the data and the IEBGENER program to write it to a data set. An organization is expected to perform regular backups of this log data to a centralized cold storage or warm storage location as part of general z/OS administrative duties.

SMF and SYSLOG data can be stored on a virtual direct-access storage device (DASD) in the Operational Environment. Virtualized DASDs are encrypted using native z/OS encryption, which protects any off-site storage of audit data. Transmission of audit data to the Operational Environment will occur within the local system so the trusted channel used to protect this data as it goes outside the TOE boundary is provided by inter-process communication and not a secure network protocol.

Any offsite backup/storage of audit data is a function initiated on the z/OS system and is not handled by ACF2. For example, the SYSLGSVW job can be used to copy the weekly SYSLOG data to tape and empty its local contents.

8.3 Communications

8.3.1 [AC]FCO_NRR.2:

In addition to administration for the local system, ACF2 provides the ability to simultaneously configure multiple systems using the Command Propagation Facility (CPF). The NODEDEF record maintained by ACF2 defines remote CPF nodes and whether they are authorized to issue commands to and/or receive commands from the system where the NODEDEF record is located. External communications are facilitated by the communications component called CAICCI, which is a part of the environmental CA Common Services component. CAICCI automatically queues any commands that were issued by CPF while a destination node is unavailable so that the command can be re-issued when the node becomes available.

All commands issued via CPF are first issued to the local system and if the command fails locally, they will not be transmitted via CPF. The CPF journal identifies, for each command that is processed by a remote node, the SYSID value of the node and the ruleset that was modified by the CPF command. This provides a record of what commands were processed by remote CPF nodes and serves as a receipt for the transaction. This identifying information also allows the remote node to use the SYSID value to identify that it is the valid recipient for the modification of a ruleset. When a command is issued interactively via CPF, the administrator receives immediate feedback in the form of a notification whether or the command was successfully processed.

The TSF can be configured to handle CPF in either synchronous or asynchronous mode using the CPFWAIT and NOCPFWAIT options. If the TSF is configured to be in synchronous mode (CPFWAIT), a CPF command that is issued interactively will prevent additional interactive commands from being entered until the initial command has been processed on all target nodes. If the TSF is configured to be in asynchronous mode (NOCPFWAIT), a command will be executed locally and on any remote nodes that are available. Any commands that are not successfully transmitted to a remote node are queued by Common Services, which in the evaluated configuration will retry the transmission every minute until the node becomes available, at which point all missed commands are transmitted in order. While this is occurring, additional commands can be executed on the nodes that are available.

An administrator can check the general status of CPF at any time using the ‘show CPF’ command.

8.4 User Data Protection

8.4.1 [AC]FDP_ACC.1(1):

CA ACF2 is deployed to control access to a variety of objects on one or more z/OS mainframe systems in the Operational Environment. The access control policy that is enforced by the TSF is made up of a collection of access control rules. These rules define the subject-object-operation combinations that are mediated by ACF2.

At their most basic level, rules are comprised of environment and access permission data. The environment defines the subject and object to which the rule applies. The subject can be a component of a UID, role, or username. A user's UID is a combination of their username and other fields in their logonid record which include organizationally defined data such as location code. Writing a rule where the subject identity includes UID data allows for administrators to write a rule against a UID that affects multiple users based on logonid record data that they share, such as an identifier for a geographic location or department.

Objects include system resources such as datasets (filesystem objects), programs, and operator commands. Table 8-2 defines the full list of behavior in the evaluated configuration as it corresponds to what is required by the AC PP for host-based access control. Masking can be used to allow for wildcards for both subjects and objects. Access permission represents the operations that the rule applies to and includes read, write, allocate (create), and execute operations. For each operation, the rule can be defined to allow (without logging), log (while allowing), or prevent (with logging) that operation.

The mainframe itself functions as the authentication server for defining users. Once a user has been authenticated to the system, ACF2 builds their logonid record which contains their username, UID, and security attributes. It also builds the user's role table to list their role associations. As the user performs actions on the system, applicable rules will use relevant portions of the user's subject data to determine whether their actions should be allowed. In this manner, all accounts on the system can be controlled.

8.4.2 [AC]FDP_ACC.1(2):

The purpose of ACF2 is to prevent unauthorized system access. This assumes that users on the mainframes within the enterprise are not trusted. Therefore, they may attempt to circumvent access control policy enforcement by terminating an instance of ACF2, altering its behavior, or preventing it from loading on system startup. To protect against this, ACF2 operates in a deny-by-default posture when operating in Abort mode. If there is no rule that explicitly authorizes an operation to be performed, it will be rejected. This includes the modification of files as well as the execution of programs and system commands. This ensures that by default, ACF2 cannot be modified or bypassed by untrusted subjects.

8.4.3 [AC]FDP_ACF.1(1):

The access control SFP controls access to different operations depending on the type of object being accessed. There are two types of rules that can be enforced by the access control SFP—access rules and resource rules. Access rules define the ability of subjects to interact with datasets and resource rules define the ability of subjects to interact with other objects on the system such as the authentication function, programs, and commands. Table 8-1 provides a summary of what is used to define the access control SFP as specified in the AC PP.

Object/Rule Type	Summary
APPLID	Application name. The access control SFP can be used to restrict system entry to authorized VTAM applications.
DATASET	Defines one or more filesystem objects.
FACILITY	A general check for various system operations, such as catalog operations.
OPERCMDS	Defines one or more operator commands, or the ability to manipulate system configuration.

PGM	Defines one or more programs by name. A resource rule can be written to have ACF2 perform an access check for a program by name when a user attempts to execute it.
RESOURCE	General term for rules that control access to system objects other than datasets. Includes pgm, opercmds, and facility.
SHIFT	Defines a repeating time over a weekly duration. SHIFT can be used to grant users access to the mainframe only during their designated shift.
SURROGAT	Defines the ability for a user to submit a job that runs under another person's logonid without the submitter knowing the execution logonid's password. This is analogous to a UNIX sudo operation.
ZONE	Defines a consistent time zone to be used when applying time-based rules so that automatic conversion to local time is performed.

Table 8-1: Command Types Summary

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

Subject	Object	Operation	Command Type
Mainframe User or Started Task	Processes	Execute	DATASET RESOURCE (PGM) SURROGAT
		Delete	DATASET
		Terminate	RESOURCE (OPERCMDS)
		Change Permissions	DATASET
	Files	Create	DATASET
		Read	
		Modify	
		Delete	
		Change Permissions	
	Host Configuration	Read	DATASET RESOURCE (OPERCMDS) RESOURCE (FACILITY)
		Modify	
		Delete	
	Authentication Function	Login	APPLID SHIFT ZONE

Table 8-2: Access Control SFP

In general, system activity is processed by the CA SAF router where ACF2 determines whether any rules apply to the activity. Once ACF2 has processed the request, the activity is either blocked or routed to the operating system where it can be completed. The TSF defines the following concepts for default rule enforcement:

- Time zone and shift data is used to govern when a user can log in to the system.

- A user must be requesting access to the system using an application (APPLID) that they are authorized to be using.
- Rules can contain masking values or wildcards that can group subjects or objects together.
- The subject data used to identify a user can be their username, their UID (which may include pertinent data from their logonid record), and/or their group memberships.
- A rule can specify different levels of authorization for different operations.

ACF2's rule processing engine determines all rules that apply to a particular requested operation and applies a rule selection algorithm to determine the most applicable rule in the event of a conflict. This works by first applying rules for the object from most specific to most general. After this, user data is processed in alphabetical order, followed by group data, followed by source data.

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

- A SECURITY user has global read/write access and READALL user has global read access for all objects except for those that have the RULEVLD (dataset) or RSRCVLD (other resource) attribute. Objects with these attributes do not bypass SECURITY/READALL checking.
- A user with NON-CNCL has global read/write access that cannot be overridden by RULEVLD/RSRCVLD.
- A SAFDEF can be defined to bypass rule checking to always arrive at a predetermined result. This can be used to unconditionally allow or deny access.
- By default, a user can access objects that they own even if there are no rules that permit that access. Ownership of an object is conferred by the high-level qualifier of an object being the same as the user's logonid.

8.4.4 [AC]FDP_ACF.1(2):

ACF2 is an executable program that resides on a z/OS mainframe. The mainframe stores ACF2's executable code as well as the VSAM databases where subject and policy data is stored and any instructions to start ACF2 that are defined as part of the system's initial program load (IPL) process. The self-protection SFP exists to ensure that an untrusted user cannot terminate, reconfigure, or otherwise bypass ACF2, including any attempts to reboot the system in a way that causes ACF2 to not be started.

ACF2 enforces the self-protection SFP on itself because all resource checks, including operator commands, are always enforced. This SFP is the deny-by-default policy that is implemented for dataset and resource access. This ensures that an untrusted user cannot bypass enforcement of the access control SFP by modifying or terminating the ACF2 software. This includes ACF2 itself as well as the databases it uses to define subject, rule, and configuration data.

8.5 Identification and Authentication

8.5.1 [PM]FIA_AFL.1:

ACF2 defines a global system option (GSO) PSWD record that defines administrative controls related to administrator passwords. One of these values is called PASSLMT and defines the maximum number of failed login attempts an administrator can make before their account is suspended. By default, this value is 2, but it can be set to a maximum of 32,767. The TSF tracks the number of authentication failures that come from attempted use of password credentials (PSWD-VIO) as well as password phrase credentials (PWP-VIO). A violation occurs when PSWD-VIO plus PWP-VIO exceeds PASSLMT. Once the account is suspended in this manner it is locked out until an administrator manually unlocks the user with the RESET or RESETPWP operator command. The violation count is reset daily or when the user account is unlocked.

8.5.2 [PM]FIA_USB.1:

Users of the TOE are associated with pertinent subject security attributes through their logonid record. These subject security attributes determine the extent to which they can manage the TSF. The logonid record is the primary source where an administrator is associated with their subject attributes. Specifically, ACF2 will control access to its management functions by examining two fields in the logonid record: the logonid itself and the privileges field. The privileges field defines the administrative role(s) (as defined in **[AC+PM]**FMT_SMR.1) that are associated with the user. These roles define the operations that are available to the user. If the user has any of these roles other than USER, the Security Target defines them as an administrator.

In addition to privileges, an administrator can also be associated with scope records. Scope records limit the objects that they are authorized to administer. For example, an administrator with the ACCOUNT role could have a scope record that limits their administrative authority to only the logonid records that belong to a certain department, geographic region, or some other administratively-defined filter. Scope records are associated with administrators based on their logonid, which is why the logonid component of the logonid record is a security-relevant subject security attribute for administrators.

The administrator’s logonid record and scope records are constructed at system entry. By default, any change to this information will not take effect until the administrator logs out and logs back in. In addition, the records must be rebuilt after the change occurs.

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

8.6 Security Management

8.6.1 [PM]FMT_MOF.1:

The TSF provides for the ability to perform internal management functions. Fundamentally, these functions typically involve the querying and/or manipulation of one or more of the Logonid, Infostorage, or Rule databases within the ACF2 Security Database. By default, SECURITY users can manipulate Rule and Infostorage data, while ACCOUNT and LEADER users can manipulate Logonid data. An ACCOUNT user must also have the SECURITY role assigned to them to manipulate Logonid data related to SECURITY users. AUDIT users can query any data but cannot modify it, while CONSULT users can query only Logonid data. When CPF is used, the administrator issuing a command must have a logonid record defined on the remote node(s) with appropriate privileges for the command to be authorized. In other words, the permissions they have on the originating system are not inherited by the remote nodes and the TSF does not assume a different role on their behalf. A mapping of the default authorized role(s) for each security function is provided in Table 6-4.

Administration of the access control SFP can be centralized or decentralized in terms of authority. If configured to be centralized, only an administrator explicitly defined as SECURITY can write access rules. If decentralized, an object owner can write rules for objects that they own, effectively allowing them to serve as a SECURITY administrator with a scope that is limited to those objects. A user can also be given the ability to change a rule set by its creator using the %CHANGE and %RCHANGE options in the rule set. A SECURITY administrator can set whether administration is centralized or decentralized. The terms centralized and decentralized refers specifically to who has the authority to write access rules; an environment where multiple systems are managed using CPF can be administered in either a centralized or decentralized manner.

Note that these represent the default privileges that are associated with each role out of the box by ACF2. There are two ways to alter the behavior that is described in Table 6-4, as follows:

- Modification of the ACF Field Definition Record (ACFFDR) can modify the privileges that are assigned to each role.
- Scope rules applied to individual administrators can prohibit them from performing authorized functions against certain objects. For example, an ACCOUNT administrator could be restricted to only have the ability to modify logonid records that matched a field in their own UID.

The environmental CA LDAP Server product can be used to translate LDAP queries on user data into equivalent commands that are recognized by CA ACF2, which are then executed as if a human administrator was issuing them via TSO. The remote LDAP directory will log in to CA LDAP Server to transmit these queries. This process associates the LDAP directory with a logonid of its own so that the directory has the appropriate authority needed to configure the user data.

8.6.2 [AC]FMT_MOF.1(1):

The TSF provides the ability to manage the functions of its access control enforcement mechanism. The following lists the functions defined by the SFR and describes how they are managed in a way that their associated SFRs are satisfied:

Audited events ([AC]FAU_SEL.1) - The auditable events that are actually audited by ACF2's access control functionality are dependent on the configuration of the rules that are being enforced. By default, logs will be generated for all access attempts that are rejected by a rule. Rules that are written using the ALLOW parameter will not generate logs when they authorize requests but rules that are written using the LOG parameter will both authorize the request and generate a log. Additionally, logging can be enabled or disabled for individual operations within a rule. Alternatively, if the TRACE attribute is enabled for a user, all activities performed by that user will be logged regardless of how the rules are defined.

Repository for remote audit storage ([AC]FAU_STG_EXT.1) – This is not applicable to the TSF because ACF2 is automatically configured to write its audited events to SYSLOG and SMF, which is the expected behavior for the remote audit storage function.

Access Control SFP ([AC]FDP_ACC.1(1)) – ACF2 can be set into different operational modes by a SECURITY user that fundamentally alter the behavior of the access control enforcement mechanism against dataset objects. In the evaluated configuration, the TOE is set into Abort mode, which is the mode in which access control policy rules will prevent unauthorized actions from being performed.

The SECURITY administrator can affect the access control SFP behavior without taking the TOE out of its evaluated configuration by defining access control rules that grant users permissions to interact with certain objects on the system.

Policy being implemented by the TSF ([AC]FDP_ACF.1) – Because ACF2 only has a single policy, management of this function is synonymous with modifying the rules and rule sets that are active on the system. This is performed by a SECURITY administrator or someone who is acting in that capacity as per [PM]FMT_MOF.1.1.

Access Control SFP behavior to enforce in the event of communications outage ([AC]FPT_FLS_EXT.1) – By default, ACF2 does not require an active communications channel to a policy origin point to enforce the access control SFP as defined. For example, if a CPF node loses connection to the system where the CPF commands originated, the loss of connectivity will not affect the ability of the node to enforce the rules that it has already received. Therefore, this function is not applicable.

8.6.3 [AC]FMT_MOF.1(2):

Administrators can see the current policy rules that are implemented by ACF2 on the local system using the “show” command. The Node Descriptor Table (NDT) on both sides of the transactions identifies the authorized senders and receivers of CPF commands for each system. Within an organization, a system will be uniquely identified via SYSID and its authenticity will be validated using shared certificates that are created, managed, and exchanged by ICSF and Common Services in the Operational Environment.

8.6.4 [PM]FMT_MOF_EXT.1:

The functions a Policy Management component is required to modify for an Access Control component are identical to the set of functions defined in [AC]FMT_MOF.1(1). Refer to section 8.6.2 for the administration functions ACF2 can perform against its access control enforcement capability and the roles that are privileged to administer those functions.

8.6.5 [AC]FMT_MSA.1:

ACF2 can administer access control policies, both on the local system on which it is installed and on remote systems using CPF. This includes the policies themselves and any attributes that are used to govern the enforcement of access control policies such as individual rules and subject attributes.

In all cases, the access control policies being managed are enforced by ACF2 so there are no issues with compatibility since both management and enforcement are done by the same product. Regarding authorizations, the NDT describes authorized senders and receivers of CPF commands. Additionally, an administrator on the local system is given privileges based on their assigned role attributes restricted by any scope rules applied to their logonid. If an administrator issues a command using CPF, their authorization on the remote system is determined by how they are defined by the target system, which may differ from the originating system if logonid records are not replicated across distributed systems.

8.6.6 [AC]FMT_MSA.3:

By default, ACF2 enforces restrictive default values for access control enforcement. If ACF2 is set in Abort mode in accordance with the evaluated configuration, access to an object is not granted unless a rule specifically allows it. An administrator can override these restrictive default values by writing permissive rules.

8.6.7 [PM]FMT_MSA_EXT.5:

The TOE's policy definition engine does not allow for the definition of ambiguous policies. Based on the way that ACF2 uses policy data to control access to the system, there are several types of potential inconsistencies that could arise, such as:

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

These inconsistencies are resolved automatically through the following precedent rules:

- Rules are processed by level, with all rules in each level taking precedence over all rules in a lower level. The relevant rule levels in order from highest priority to lowest are: DSN (dataset name), VOL (volume), UID, SOURCE, PGM, and SHIFT. There are additional levels within ACF2 but those shown here are sufficient to describe the access control SFP as prescribed by the AC PP.
- DSN, VOL, and UID rules are applied from most specific to most general. In other words, a rule for a specific dataset will take precedence over a rule matching only the dataset's high level qualifier. Similarly, a rule that matches the literal subject or object name will take precedence over a rule that matches a mask or wildcard.
- SOURCE and SHIFT operands are applied in alphabetical order. For example, a SHIFT record named "ABNORMAL" will take priority over one named "NORMAL".

For rules where a duplicate security environment (identical subjects, objects, and operations) is defined, ACF2 will throw an error when an attempt to compile the ruleset is made. This prevents the definition of ambiguous policies where duplicate sets of activities are given different levels of privilege by different rules.

The NOSORT GSO record will cause rules to be processed in the order in which they were entered, disregarding the processing hierarchy described above. This option is not recommended.

For rules to be understandable to ACF2, a compile instruction must be issued to convert the rule data into a machine-readable format. During this process, the appropriate rule ordering is determined based on the processing hierarchy described above.

8.6.8 [AC+PM]FMT_SMF.1:

ACF2 provides administrators with the ability to manage all necessary aspects of the TSF where applicable. The following table provides a high-level description of the method by which each of the activities are performed. Refer to section 8.6.1 for an overview of the privileges required to perform these activities.

SFR	Management Activity	Managed By
[PM]ESM_ACD.1	Creation of policies	Access rules, resource rules
[PM]ESM_ACT.1	Transmission of policies	CPF
[PM]ESM_ATD.2	Association of attributes with subjects	Logonid records
[PM]ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Logonid records
[AC+PM]ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Logonid records
[PM]FAU_SEL_EXT.1	Configuration of auditable events for defined external entities	Access rules, resource rules
[PM]FAU_STG_EXT.1	Configuration of external audit storage location	N/A – external audit storage is the local operating system's SYSLOG and SMF audit logs
[PM]FIA_AFL.1	Configuration of authentication failure threshold value	GSO records
	Configuration of actions to take when threshold is reached	N/A – when the threshold is reached, the logonid is automatically locked until manually reset by an administrator
	Execution of restoration to normal state following threshold action (if applicable)	Logonid records
[PM]FIA_USB.1	Definition of subject security attributes, modification of subject security attributes	Logonid records
[PM]FMT_MOF_EXT.1	Configuration of the behavior of other ESM products	Access rules, resource rules, GSO records
[PM]FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)	GSO records
[PM]FMT_SMR.1	Management of the users that belong to a role	Logonid records
[PM]FTA_TAB.1	Maintenance of the banner	N/A – the Operational Environment is responsible for displaying the banner, which is appropriate as per NIAP TD0055
[AC+PM]FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	CPF (note that the TOE will always use the trusted channel for CPF communications if the Operational Environment is configured to facilitate this but CPF configuration allows an administrator to specify the remote endpoints for this channel by identifying the SYSIDs that receive CPF commands)

[PM]FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	N/A – the TOE will always use the trusted path for remote administration if the Operational Environment is configured to facilitate this

Table 8-3: TSF Management Functions by Activity

8.6.9 [AC+PM]FMT_SMR.1:

In terms of defining what administrative actions are available to an administrator, ACF2 provides several default roles out of the box, listed below:

- ACCOUNT – ability to manage logonid records for any user except for those with SECURITY privilege (unless the administrator has both SECURITY and ACCOUNT privileges).
- AUDIT – ability to view logonid records, infostorage records, and rules.
- CONSULT – ability to view logonid records for non-administrative users.
- LEADER – ability to view logonid records for non-administrative users and manage an administrator-defined set of fields within these records.
- SECURITY – ability to view and manage all system data not related to logonid records.
- USER – ability to view their own logonid record.

The ‘privileges’ field in a user’s logonid record identifies which administrative role(s) they are associated with. Scope rules can be used to limit the set of subjects or objects that different administrators within a role can administer. For example, a scope rule could be written to restrict ACCOUNT role members to manage the accounts of users within their own departments (as defined in their extended UID). When an administrator is using CPF to configure a remote system, they must have a logonid defined on the target system with sufficient privileges to issue the command. The TSF will inherit the administrator’s privileges that are defined on a remote node when a command is issued to that node.

Note that these privileges and actions that they authorize are defined by default in the field definition record (ACFFDR). An administrator can modify this record to make site-specific customizations to the authority defined for the administrative roles, such as defining the logonid record fields that members of the LEADER role can modify.

8.7 Protection of the TSF

8.7.1 [AC+PM]FPT_APW_EXT.1:

Administrator credential data is stored in an obfuscated manner (configurable to be either AES or a DES variant known as XDES) in the Infostorage database. This database is protected from unauthorized access by ACF2. Password and password phrase data can be encrypted by the environmental ICSF component using the PSWDENCT GSO setting. The claimed Protection Profiles do not require a specific method of obfuscation so either setting is permitted in the evaluated configuration. Note that it is possible for batch jobs to store username/password data on the job card. While this data is not stored by the TSF, it could be used to subvert the TOE’s access control policy if compromised. It is therefore recommended that use of this be limited to essential situations and that care is taken to ensure that the TSF is configured to prevent unauthorized users from accessing any job cards that store credential data.

8.7.2 [AC]FPT_FLS_EXT.1:

If ACF2's use is limited to a single mainframe system, there is no situation in which its policy management capability will be unable to communicate with its access control capability since each of these capabilities read to and write from identical databases. Since the access control capability relies on stored database information to enforce the access control SFP, an active external connection is not required for it to continue to function. In the case of CPF, a node that is unable to communicate with the system that transmitted rule data to it will continue enforcing whatever rules it currently has stored until communications with the policy origin point are restored. Once this occurs, any commands that were issued during the outage are released from a queue and transmitted to the node.

8.7.3 [AC]FPT_RPL.1:

ACF2 protects against replayed data first and foremost using TLS communications between remote systems. This is provided by cryptographic services on the underlying z/OS platform. The payload of a CPF packet is encrypted and decrypted using a shared key. The entire packet, including the CPF header, is encrypted and decrypted by the transmission vehicle. Once the receiving node has decrypted the packet, the CPF header will be verified to ensure that it is a valid CPF message. This ensures that a CPF node will not receive false policy data because an attacker would need to successfully decrypt the packet, modify the data, and re-encrypt the packet. Additionally, the Node Descriptor Table defines authorized and active senders of CPF commands. The administrator who is sending the command over CPF is also defined with a certain set of privileges, so an attacker would be unable to escalate their privileges as part of a replay attack. Any attempted replay will therefore be rejected by the TSF and logged as an invalid or unauthorized command.

8.7.4 [AC+PM]FPT_SKP_EXT.1:

ACF2 does not provide its own cryptography; instead, it relies on the ICSF component in the Operational Environment for encryption functions. Any keys used to encrypt password data or establish SSH or TLS secure communications are stored within ICSF and not maintained by the TSF.

8.8 Resource Utilization

8.8.1 [AC]FRU_FLT.1:

ACF2 will enforce the consumed access control policy regardless of whether it can communicate with the source of its policy. This is because each instance of ACF2 includes its own access control enforcement mechanism that is identical to each other instance. In a case where CPF is being used to manage a remote node and the remote node loses connectivity to the source of its policy data, there will be no impact on that node's ability to enforce the access control policy rules it already has. Any CPF commands that are issued by the originating node will be queued and it will periodically attempt to contact the remote node. Once connectivity has been restored, the queued CPF commands will be transmitted in their original order to the remote node. CPF on the sending node can be configured to be in either synchronous or asynchronous mode. In synchronous mode, the sender cannot process any further commands until the queue is empty. In asynchronous mode, additional commands can be entered on the local system and any responding nodes without requiring the queued commands to be processed first. Regardless of how the sending node is configured, the recipient of the CPF commands will behave the same way if communications between the two are interrupted.

8.9 TOE Access

8.9.1 [AC+PM]FTA_TSE.1:

As part of the requirements for Host-Based Access Control, the TSF is required to allow or deny access to the login function of the system on which its access control functionality resides. In the case of ACF2, this means that it must control whether a user is permitted to log in to the mainframe system. At minimum, this is for blanket allow/deny access.

In addition to this, the AC PP provides an optional SFR that allows for the definition of conditional access to the login function. The TSF claims this SFR and specifies that conditional access is based on day and/or time. As described in **[AC]**FDP_ACF.1(1), ACF2 can define SHIFT records for users. These records define the times that a user might be expected to use the system. Rules can then be written to prevent the user from authenticating during days or times that are not part of their regular shift. Additionally, authentication can be restricted based on the authorized application (APPLID). The APPLID value is defined by the application and subsequently supplied by VTAM when an OPEN is performed on the application, so it is not a value that a user can control directly. Finally, if a logonid record has the suspend flag set for it, the corresponding user will not be able to log in.

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

8.10 Trusted Path/Channels

8.10.1 [AC+PM]FTP_ITC.1:

ACF2 can communicate with remote systems over TCP/IP for the purposes of executing remote commands using CPF. This connection occurs over a TLS protected channel between the different mainframe systems. TCP/IP communications are facilitated by CA Common Services, which invokes IBM’s ICSF and System SSL components to establish trusted communications using TLS. These components use the following CAVP-validated algorithms to establish TLS communications:

ICSF:

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

System SSL:

- AES conformant to FIPS PUB 197 and NIST SP 800-38A: certificate #4083
- RSA conformant to FIPS PUB 186-4: certificate #2210
- SHS conformant to FIPS PUB 180-4: certificate #3361
- HMAC conformant to FIPS PUB 198-1: certificate #2665

In the evaluated configuration, System SSL is configured to invoke ICSF for DRBG and Diffie-Hellman services since its own random number generator has been deprecated. ACF2 indirectly initiates all communication via the trusted channel by invoking CA Common Services. CA Common Services then interfaces with System SSL and ICSF as needed to secure remote TLS communications.

8.10.2 [PM]FTP_TRP.1:

As a mainframe application, ACF2 does not provide a separate interface for remote access. Administrators will access the mainframe system using a TN3270e terminal emulator. Administrators will use an SSH-capable client to access the mainframe system, which will handle these communications with OpenSSH for z/OS. In the evaluated configuration, OpenSSH for z/OS is configured to invoke ICSF for all cryptographic primitives that require CAVP validation. ICSF uses the following CAVP-validated algorithms to assist in the establishment of SSH communications.

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