National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

CA ACF2™ r14 SP1 for z/OS

Report Number: CCEVS-VR-VID10416-2011
Version 1.1
April 4, 2011

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

1 Executive Summary

The Security Target (ST) defines the Information Technology (IT) security requirements for CA ACF2 for z/OS (CA ACF2). CA ACF2 delivers access control capabilities for z/OS systems and includes interfaces for CICS, TSO, and IMS. CA ACF2 allows administrators to control user access to protected mainframe resources such as datasets and volumes. CA ACF2 controls access to the system and its own data through the use of policies and privileges that limit how and when a user or administrator can access the system and what they can do once they are authenticated. Administrators can be given authority over various segments of the system through the use of scope records.

2 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product	CA ACF2 r14 SP1 for z/OS
Sponsor & Developer	CA Technologies, Lisle IL
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	March 2011
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL4 Augmented ALC_FLR.1 and ASE_TSS.2
Description	The TOE is the CA ACF2 software, which is a security product developed by CA Technologies as a System Access Control product.
Disclaimer	The information contained in this Validation Report is not an endorsement of the CA ACF2 product by any agency of the U.S. Government, and no warranty of the product is either expressed or implied.
PP	None.
Evaluation Personnel	Ronald Ausman Justin Fisher Paul Juhasz Arthur Leung Derek Scheer Amit Sharma

Validation Body	NIAP CCEVS

2.1 Threats to Security

Table 2 summarizes the threats that the evaluated product addresses.

Table 2 – Threats

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

3 Identification

The product being evaluated is CA ACF2 r14 SP1

4 Security Policy

4.1 Security Audit

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

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

4.2 Identification & Authentication

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

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

4.3 Security Management

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

The SECURITY, ACCOUNT, and AUDIT privileges are the most commonly used in reference to being assigned to the users and administrators. An administrator has the SECURITY privilege assigned to their User ID record. This privilege will allow the administrator to perform management actions and view audit records within their scope. Any administrator with ACCOUNT administrative authority can create users/administrators. On the other hand, either a user or administrator can have the AUDIT privilege defined in their User ID record. This allows the user or administrator to display any audit record, and are considered to be an auditor.

4.4 User Data Protection

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

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

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

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

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

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

4.5 TOE Access

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

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

5 Assumptions

5.1 Physical Assumptions

Table 4 – Physical Assumptions

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

5.2 Personnel

Table 5 – Personnel Assumptions

One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.
Administrators exercise due diligence to update the TOE with the latest patches and patch the Operational Environment so they are not susceptible to network attacks.
Administrators of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.

6 Clarification of Scope

The TOE includes all the product code and SAF code (shared libraries with CA Top Secret) which pertain to the security requirements defined in the ST.

The evaluated configuration of the TOE necessitates that it be running in ABORT mode. Any other configuration parameters are at the discretion of site administrators within the bounds of any organizational policies defined for the site. For example, the TOE has a configurable password policy. No prescription is made by the evaluation laboratory regarding its configuration. An administrator is expected to configure the password policy in accordance with site requirements or, in the absence of these, reasonable security best practices.

6.1 Physical Boundary

The TOE includes the CA ACF2 components:

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

The following z/OS requirements are pre-requisites to the installation of the TOE. Note that these requirements are also pre-requisites for z/OS functioning properly so in the event of an incremental install, the presence of a previous version of CA ACF2 is sufficient to ensure that these OS requirements were met.

Requirement	Description
An Operating System	z/OS V1R9 or later
A TSO/E Session	A TSO/E Session on the IPLed system must be established using a locally-attached or network-attached terminal
Proper Security	In order to install the z/OS UNIX files, the following is required: • The user ID must be a superuser (UID=0) or have read access to the BPX.SUPERUSER resource in the SAF FACILITY class. • The user ID must have read access to FACILITY class resources BPX.FILEATTR.APF, BPX.FILEATTR.PROGCTL, and BPX.FILEATTR.SHARELIB (or BPX.FILEATTR.* if a user chooses to use a generic name for these resources). The commands to define these FACILITY class resources are in SYS1.SAMPLIB member BPXISEC1. • Group IDs uucpg and TTY, and user ID uucp, must be defined in the security database. These IDs must contain OMVS segments with a GID value for each group and a UID value for the user ID. (For ease of use and manageability, define the names in uppercase.)
OMVS Address Space Active	For ServerPac only (not SystemPac), an activated OMVS address space with z/OS UNIX kernel services operating in full function mode is required.
SMS Active	The Storage Management Subsystem (SMS) must be active to allocate

	z/OS UNIX file systems (HFS or zFS) and PDSE data sets, whether they are SMS-managed or non-SMS-managed. Also, the use of z/OS UNIX file systems (HFS or zFS) is supported only when SMS is active in at least a null configuration, even when the file systems are not SMS-managed. Do either of the following: • To allocate non-SMS-managed z/OS UNIX file systems (HFS or zFS) and PDSE data sets, a user must activate SMS on the driving system in at least a null configuration. A user must also activate SMS on the target system. • To allocate SMS-managed z/OS UNIX file systems (HFS or zFS) and PDSE data sets, A user must activate SMS on the driving system in at least a minimal configuration. Then a user must define a storage group, create SMS-managed volumes, and write, translate, and activate a storage class ACS routine that allows the allocation of z/OS UNIX file systems (HFS or zFS) and PDSE data sets with the names in the ALLOCDS job. A user must also activate SMS on the target system.
DFSORT	msys for Setup job XMLGNR8 requires DFSORT or an equivalent sort program on the system on which the XMLGNR8 job is run.
Language Environment Requirements	The CustomPac Installation Dialog uses the Language Environment run-time library, SCEERUN. If SCEERUN is not in the link list on the driving system, a user must edit the ServerPac installation jobs to add it to the JOBLIB or STEPLIB DD statements.
CustomPac Installation Dialog	If installing a ServerPac or dump-by-data-set SystemPac for the first time, a user will need to install the CustomPac Installation Dialog on the driving system. See *ServerPac: Using the Installation Dialog* or *SystemPac: CustomPac Dialog Reference* for instructions. For subsequent orders a user will not need to reinstall the dialog. IBM ships dialog updates with each order. A user can check the PSP bucket for possible updates to the CustomPac Installation Dialog. For ServerPac, the upgrade is ZOSV1R11 and the subset is SERVERPAC. For SystemPac dump-by-data-set orders, the upgrade is CUSTOMPAC and the subset is SYSPAC/DBD.
Proper Level for Service	In order for a user to install service on the target system that they are building, a user's driving system must minimally meet the driving system requirements for CBPDO Wave 1 and must have the current (latest) levels of the program management binder, SMP/E, and HLASM.
SMP/E ++JAR Support	If the ServerPac order contains any product that uses the ++JAR support introduced in SMP/E V3R2 (which is the SMP/E in z/OS V1R5), the driving system requires IBM SDK for z/OS, Java 2 Technology Edition, V1 (5655-I56) at SDK 1.4 or later. z/OS itself does not use the ++JAR support.
zFS Configured Properly	If using a zFS for installation, then a user must be sure that the zFS has been installed and configured, as described in *z/OS Distributed File Service zSeries File System Administration*.
Internet Delivery Requirements	If intending to receive the ServerPac or SystemPac dump-by-data-set order by way of the Internet, a user will need the following: • SMP/E PTF UO00678 (APAR IO07810) if SMP/E level is V3R4 (which is in z/OS V1R7, V1R8, and V1R9). v ICSF configured and active so that it can calculate SHA-1 hash values in order to verify the integrity of data being transmitted. If ICSF is not configured and active, SMP/E calculates the SHA-1 hash values using an SMP/E Java application class,

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

	information about using the Distributed FileManager, see *z/OS DFSMS DFM Guide and Reference*. ○ CD write capability. If specified that 100% electronic delivery is required, there might be CD images associated with the order. The images are delivered in ISO9660 format and are packaged in zip files (with an extension of .zip). These files require the workstation to have CD write capability and might have to acquire software to support this capability.

6.2 Operational Environment Components

6.2.1 Cryptographic Support

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

6.2.2 Time Stamps

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

6.2.3 Audit Storage

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

6.2.4 Application Interfaces

The TOE is able to mediate transactions initiated through various applications and facilities such as TSO, CICS, IMS, and ISPF. Programs used to access these interfaces such as a TN-3270 terminal emulator are considered to be part of the Operational Environment. CICS and IMS servers which reside on the mainframe and facilitate these transactions are also considered to be part of the Operational Environment.

6.2.5 LDAP Repository

Use of an LDAP repository to store user data is an optional capability of the TOE. If this is enabled, the repository itself resides outside the TOE boundary and is considered to be part of the Operational Environment.

6.3 Operational Environment Components

The following optional products, components, and/or applications can be integrated with CA ACF2™ r14 SP1 for z/OS but are not included in the evaluated configuration. They provide no added security related functionality. They are separated into three categories:

not installed, installed but requires a separate license, and installed but not part of the TSF.

6.3.1 Not Installed

These components are not installed with CA ACF2™ r14 SP1 for z/OS and are therefore not included in the TOE boundary. It does not matter if they are installed on the Operational Environment because they are out of scope for the requirements in this evaluation as explained below.

- **EUA** – Extended User Authentication (EUA) can make a requirement for some users to be processed for additional authentication beyond the normal CA ACF2 User ID and password validation, and enables other users to sign on without further user authentication. Including this functionality requires a third party product, and additional software that is plugged into a CA ACF2 optional component for use with Tokens / Common Access Cards.
- **ELM Integration -** Enterprise Log Manager (ELM) allows Administrators to collect, normalize, aggregate, and report on security relevant activity, and generate alerts requiring action when possible compliance violations occur. It has no security impact on the TOE and is not included in the evaluated configuration of the TOE.
- **CA Compliance Manager for z/OS Integration** – CA Compliance Manager for z/OS allows Administrators to collect, and report on security relevant activity, and generate alerts requiring action when possible compliance violations occur. It has no security impact on the TOE and is not included in the evaluated configuration of the TOE.
- **CA ACF2™ Option for DB2 UDB** – CA ACF2 Option for DB2 UDB is outside the scope of the evaluated configuration because it has no security impact on the TOE and is excluded from the evaluated configuration.
- **DFSMS** – DFSMS is an IBM designation for the DF/HSM, DFDSS, DFSORT, DFRMM, and RACF products when used in a DFSMS system. It is not a necessary component for CA ACF2 because the TOE contains its own databases to perform the same functionality.

6.3.2 Installed but Requires a Separate License

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

6.3.3 Installed But Not Part of the TSF

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

- **Group** – CA ACF2 only validates the use of the GROUP parameter if the user specifies a group that is not the default specified in his User ID record. This functionality is not commonly used for the current functions of the TOE, and is only supported by the TOE for backward compatibility. The functionality provided by Group is not used for object access by the TOE.

- **UADS or No UADS (User Attribute Data Set)** – Obsolete and can be shut off. Not part of the evaluated configuration. The advantages of bypassing UADS are faster logon processing and eliminating the need to maintain both UADS and the User ID database.

- **SYSPLEX** – The coupling facility is a feature of z/OS that allows systems in a sysplex environment to communicate and share data with each other. It allows multiple systems to share one security file. Security in a sysplex environment is based on:

    - The communication function or Cross System Coupling Facility (XCF) that provides a way for each system in the sysplex to send messages or signals to all other systems.

    - The data sharing function or Cross System Extended Services (XES) that provides the ability for systems in the sysplex to share common data that would normally be obtained from a database. This function saves system resources by reducing I/O to the database.

- **Security Modes** – The following security modes are not security enforcing and are therefore not included in the evaluated configuration:
    - Rule Mode – Lets the TOE validate rules for different data sets in different modes while the site is migrating to full security. CA ACF2 checks for a $MODE statement in the rule set when it validates an access request. If there is no $MODE statement in the rule set or if no rule set exists, the system-wide mode specified determines how access rules are processed.

    - Quiet Mode – Accesses are not validated or logged. Logonid, source, and other validations still take place. A site can use this mode until they have written basic access rules for the system to reduce the number of access violations logged.

    - Log Mode - Logs access violations, but allows access. A user can use this mode after they have written basic access rules to generate access violation reports and determine what access rules still need to be written.

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

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

7 Architectural Information

The TOE's boundary has been defined in Figure 1.

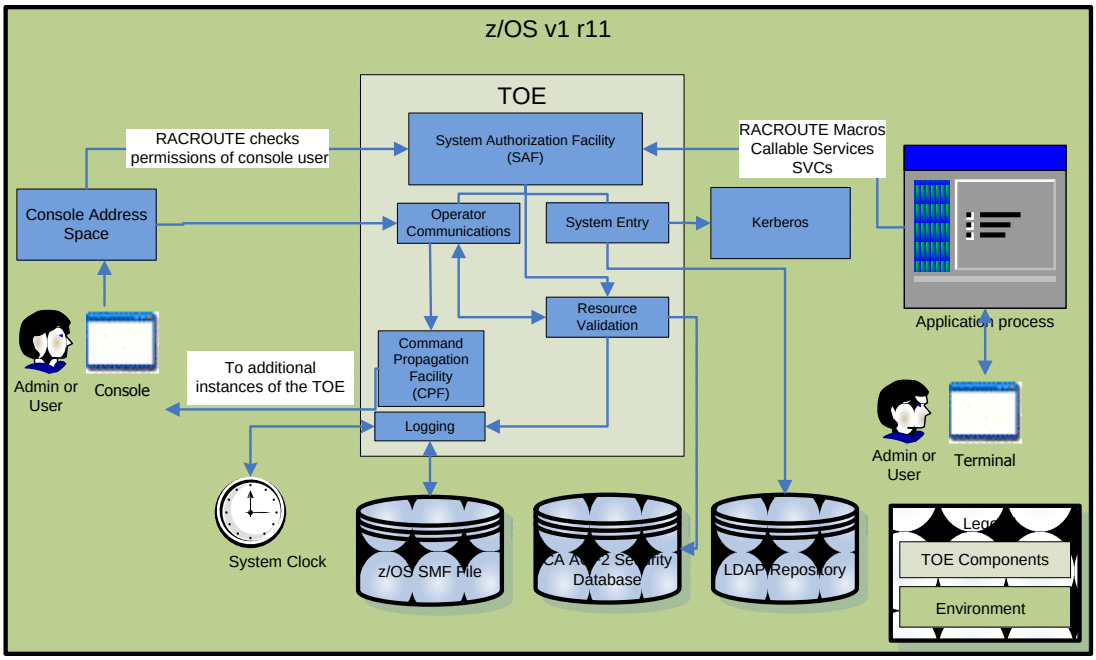

Figure 1 – TOE Boundary for CA ACF2 r14 SP1

8 TOE Acquisition

The NIAP-certified ACF2 product is acquired via normal sales channels. Delivery of the TOE to the customer site is accomplished one of two ways:

- For sites with mainframes that have direct internet access, the CA Mainframe Software Manager (MSM) program can be used to acquire the TOE from CA's site using FTP.
- For sites with mainframes that do not have direct internet access, the CA software package (.pax file) can be acquired using a system which is able to access the internet and subsequently using FTP within the installation's firewall or Cross-Domain Solution to transfer the package to the mainframe and subsequently use CA MSM to install the package.

The following documents are provided with the TOE:

- CA ACF2 for z/OS Administrator Guide

- CA ACF2 for z/OS Auditor Guide
- CA ACF2 for z/OS Best Practices Guide
- CA ACF2 for z/OS CICS Support Guide
- CA ACF2 for z/OS Command Reference Guide
- CA ACF2 for z/OS Compliance Information Analysis Guide
- CA ACF2 for z/OS Cookbook
- CA ACF2 for z/OS Distributed Database Support Guide
- CA ACF2 for z/OS Implementation Guide
- CA ACF2 for z/OS IMS Batch Support Guide
- CA ACF2 for z/OS IMS Support Guide
- CA ACF2 for z/OS Installation Guide
- CA ACF2 for z/OS Message Reference Guide
- CA ACF2 for z/OS Multi-Level Security Planning Guide
- CA ACF2 for z/OS Quick Reference Guide
- CA ACF2 for z/OS Release Notes
- CA ACF2 for z/OS Report and Utilities Guide
- CA ACF2 for z/OS Reporting with CA Earl Guide
- CA ACF2 for z/OS Systems Programmer Guide

Of these documents, the following were reviewed by the evaluation team in order to complete the evaluation:

- Administrator Guide
- Multilevel Security Planning Guide
- Implementation Planning Guide
- Auditor Guide
- Installation Guide
- Quick Reference Guide
- Report and Utilities Guide
- CICS Support Guide
- IMS Support Guide

The remaining documents, while potentially informative to the end customer, were not examined as part of the CC evaluation.

9 IT Product Testing

The test team's test approach is to test the security mechanisms of CA ACF2 by exercising the external interfaces to the TOE, viewing the TOE's behavior, and examining the logged results. Each TOE external interface is to be described in the relevant design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), Security Architecture (ARC) and the vendor's test plans will be used to demonstrate test coverage of all EAL4 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements will be determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team will create a test plan that contains a sample of the vendor functional test suite, and supplemental functional testing of the vendors' tests. Booz Allen will also perform vulnerability assessment and penetration testing.

9.1 TEST METHODOLOGY

9.1.1 Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, the nvd.nist.gov, and Secunia. However, because of the particularities of the MVS environment, no useful information was found at these sources. The evaluators then consulted a number of mainframe-specific resources in order to determine potential attack vectors for the TOE.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.
The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network. Specifically, the evaluators examined the communications between a remote terminal application and the mainframe in order to determine if security-relevant data could be extracted. While encryption over this interface is not the TOE's responsibility, testing it helps determine the sufficiency of preparatory procedures and assumptions for the security environment.
- Disabling the TOE
  The TOE should be resistant to attempts to kill its execution or datasets which comprise it. If a utility such as AMASPZAP can be used to halt its execution, then an unauthorized user can perform unauthorized operations against the system.
- Job Entry Subsystem
  The Job Entry Subsystem is a mechanism by which the Terminal Application Process external interface to the TOE can be invoked. The TOE should be resistant to unauthorized jobs to query or update data on the system.
- Database Compromise
  This test is intended to attempt to dump database contents such as the VSAM file to look for security data which could be used to footprint the system or masquerade as another user.
- Address Dump
  This test is designed to cause a failure of a system service which would generate an SVC dump. The contents of this dump will potentially contain security data which the user reading the dump would not ordinarily be allowed to see.
- SMF Dump
  This test involves generating audit reports of system data. A lesser privileged user is typically allowed to review audit data, but there is the potential for security data to be contained within the audit reports that they could potentially use to escalate their privileges or masquerade as another user.
- System Entry/Escalation
  This test uses any security data that was identified in the previous tests in order to attempt to gain unauthorized access to either the system itself or to resources protected by the system.

9.1.2 Vulnerability Results

The Address Dump tests discovered an exposure.

Synopsis: User password information was found common storage, in VTAM trace and CPF buffers. The CPF data is transient, only in storage while CA ACF2 is processing the CPF updates. The greater vulnerability is in the z/OS (VTAM) storage, which is not under the direct control of CA ACF2. Exploitation of this vulnerability requires both elevated privileges, and a detailed knowledge of z/OS, z/OS debugging tools and techniques, and storage dump analysis.

A user's password can be found in a storage dump of a user's address space. The areas of storage in which the password are under the control of z/OS components under usual conditions are in common storage, in VTAM and CPF storage areas. These areas of storage will be dumped if a system dump is taken of an address space, and will be available for review by whomever can access and read the dump.

If the CA ACF2 command processor (ACF) is open in a user session to perform password changes, then the storage used by the ACF command to process the password change can contain user passwords while the command is open. When the user closes the command (goes back to the TSO command prompt), that storage apparently is cleared when the ACF command terminates. If a system dump is taken of the user's address space while the ACF command processor is open, the user passwords will be available in the storage used by the ACF command, and will be available for review by whomever can access and read the dump.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the CA ACF2 r14 SP1 for z/OS TOE meets the security requirements contained in the Security Target.

The criteria against which the ACF2 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the ACF2 TOE is EAL4 augmented with ALC_FLR.1 and ASE_TSS.2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in March 2011. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

11 Validator Comments/Recommendations

The validators do not have any specific comments or recommendations.

The following observations were made by the evaluation team in response to the completion of their independent testing efforts.

11.1 Configuration Documentation

The "CA ACF2 Best Practices Guide r14" defines the recommendations and secure usage directions for the TOE as derived from the evaluation.

11.2 Mitigation of z/OS VTAM Disclosure Vulnerability

The risk of exploitation can be mitigated by applying the following best practices:

- Control access to the SYS1.DUMPxx datasets
- Control access to the master and logical consoles
- Control access to z/OS debugging tools
- Ensure operator command security is implemented

These are sufficient practices to fully mitigate the Operational Environment vulnerability.

11.3 Use of secure terminal software

If accessing the TOE remotely in an environment that is not secure, it is recommended that individuals who access the mainframe system do so using secure terminal software such as QWS3270 Secure. The TOE is not responsible for data in transit between a user and the mainframe system, so proper care should be taken to ensure a trusted path is established by the Operational Environment.

12 Security Target

The security target for this product's evaluation is CA ACF2™ r14 SP1 for z/OS Security Target, Version 1.1, March 7, 2011.

13 List of Acronyms

Acronym	Definition
ACF2	CA ACF2
CC	Common Criteria
CICS	Customer Information Control System
CNF	Certificate Name Filtering
CPF	Command Propagation Facility
DAC	Discretionary Access Control
DFSMS	Data Facility Storage Management Subsystem
EAL	Evaluation Assurance Level
FDR	CA ACF2 Field Definition Record
GSO	Global Systems Option
ICSF	Integrated Cryptographic Services Facility
IMS	Information Management System
LDS	LDAP Directory Services
LID	Logon ID
MAC	Mandatory Access Control
MLS	Multi-level Security
MVS	Multiple Virtual Storage
MUSASS	Multiple User Single Address Space System
POE	Port of entry
RACF	Resource Access Control Facility
SAF	System Authorization Facility
SMF	System Management Facility
STC	Started Task Command
SVC	Supervisor Call
SYSID	System Identifier
TMP	Terminal Monitor Program
TOE	Target of Evaluation

TSC	TOE Scope of Control
TSF	TOE Security Function
TSO	Time-sharing option
UID	User Identification String

14 Terminology

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

Node	A single instance of the TOE. Synonymous with a Virtual Machine instance on the same machine.
Object	Any resource protected by the TOE.
Passticket	A method of authentication the TOE utilizes which is issued for specific session and cannot be used again once that session has ended. In order to generate a PassTicket, a user's UID string, time of day and session are needed.
Passphrase	A passphrase is a type of password that can exceed eight characters and can contain blanks.
RACROUTE	RACROUTE is a method of requesting information from the TOE. The list of requests are AUDIT, AUTH, CLASS = DATASET, DASDVOL, TAPEVOL, TSOAUTH, others, DEFINE, CLASS = DATASET, DASDVOL, TAPEVOL, DIRAUTH, EXTRACT, FASTAUTH, etc. These requests allow for resource validation, auditing, and data retrieval along with other possible request types. For more information, reference CA ACF2 for z/OS r14 Administrator Guide.
Resource	Any component of the computing or operating system required by a task. For the purposes of data protection, these resources are the objects reside on the system.
Resource Rule	A type of CA ACF2 rules that governs access to resources.
Resource Access Control Facility	RACF is an IBM program product that provides system entry, resource access control, auditing, accountability, and administrative control for the z/OS operating system.
Rule	Rules specify who can access resources and under which conditions resources can be shared.
Scope of authority	Scope of authority indicates what logical units the user has administrative control over.
Security administrator	A security administrator is primarily responsible for implementation and maintenance functions such as defining users, resources, and levels of access. The administrative authority determines what the security administrator can do.
Security file	Security files contain the Security Records that contain all user definitions, resource entitlement controls, and security control options. Generally, this refers to the three CA ACF2 security data bases: The Logonids database, the Rules database, and the Infostorage database.
Security label	Security labels classify users, data, and resources. Standard access rules and permissions still apply, but only after MAC label dominance checks determine that a user can access data and resources based on their security label and the security label of the data or resources the user wants to access.
Security validation algorithm	The Security Validation Algorithm determines whether CA ACF2 can accept or deny users' requests to use a resource.
Source or origin	Source or origin indicates the location of an access request (a terminal or reader).
Supervisor Calls (SVC)	Administrative calls for the TOE that allow for some management action. For example, SVCA is used to allow or deny a SAF request.
SYSID	A system identifier; a maximum of four characters may be specified and the value may contain an asterisk (*) for masking.
System Management Facility File	The SMF File is part of the Operational Environment and provided by z/OS for the purpose of event logging.
Time-Sharing Option	TSO enables two or more users to execute their programs at the same time by dividing the machine resources among terminal users.
User ID	The UID is a unique identification used for each accessor of the TOE to identify with when attempting to authorize.
User ID String	The UID string identifies a user to reduce the number of access and resource rules that must be written.

User	A user is the lowest User ID level in the security structure. Generally, a user can sign on via a password and initiate jobs.
Violation	A violation is an unauthorized attempt to access a protected resource.
z/OS UNIX ID	z/OS UNIX User Identifier