National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

CA Top Secret® r14 SP1 for z/OS

Report Number: CCEVS-VR-VID10415-2011
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 Top Secret for z/OS (CA Top Secret). CA Top Secret delivers access control capabilities for z/OS systems and includes interfaces for CICS, TSO, and IMS. CA Top Secret allows administrators to control user access to protected mainframe resources such as datasets and volumes. CA Top Secret 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 Top Secret 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 Top Secret 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 Top Secret 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 Top Secret® r14 SP1 for z/OS.

4 Security Policy

4.1 Security Audit

CA Top Secret uses the System Management Facility (SMF) to record all security-relevant events. These records are secured from accidental disclosure or destruction by the standard Discretionary Access Control (DAC) and Mandatory Access Control (MAC) protection mechanisms. The TOE may enforce the Mandatory Access Control (MAC) policy to objects based on users, resources, and AccessLevel, Type, Object Security Label, and Subject Security label. The TOE enforces the Discretionary Access Control (DAC) policy to objects based on users, entity, security relevant attributes control option auth, resource class name, entity name, secrec, ownership, facility, time of day, day of week, sysid, and Limited Command Facility (LCF).

CA Top Secret provides report utilities to produce reports. For example, the TSSUTIL utility report provides an audit trail of security events. A variety of parameters can be set to customize the reports.

The audit mechanism in CA Top Secret is able to create and maintain audit records of all security-relevant events, such as system entry, data access, and resource access. The system also protects the audit records from modification and accidental loss or disclosure. Audit records display the security label of the user and the security label of the data or resource that the user attempted to access.

4.2 Identification & Authentication

CA Top Secret controls how, when, and which resources a user can access. CA Top Secret requires that each end user have a valid accessor ID (ACID) and password before entering the system. An ACID can be up to eight alphanumeric characters long, which

normally corresponds with the user's system userid. The same ACID can be used for all facilities or a different ACID can be used for each facility (such as TSO, CICS, and z/VM).

By default, CA Top Secret requires that all ACIDs are password protected. A security administrator assigns the first password. The user associated with the ACID changes the password immediately (or later if they desire) when it expires. Password assignment is controlled by CA Top Secret; control option values are set and stored within CA Top Secret.

4.3 Security Management

The TOE maintains three roles: security administrators, scoped security administrators and users. Administrators manage the TOE and its users whereas a user's primary function is to perform work. Any administrator with ACID (CREATE) administrative authority can establish users.

Security administrators can display and change fields of ACIDs based on their scope.

4.4 User Data Protection

CA Top Secret enforces whether an individual user should be permitted access to a resource based on administratively-defined policy and must be able to associate a user's identity with each job or time-sharing session. No job can run on a CA Top Secret-controlled system unless it can first be identified with a valid, predefined user. Thus, CA Top Secret also protects the resources of the computer system itself. No one can use processing time on a system unless they are running under an ACID previously defined to CA Top Secret.

CA Top Secret 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 separate users, data, and resources into logical domains. 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.

DAC security policy manages the controlled sharing of data and resources using permissions. A security administrator or data owner can write rules to permit sharing. If a user tries to access data without permission, the system creates a violation record and denies access.

4.5 TOE Access

CA Top Secret will deny access to TOE users who have a suspended/canceled account or have failed to enter a correct password within the threshold limit set by an administrator.

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 ACF2) which pertain to the security requirements defined in the ST.

The evaluated configuration of the TOE necessitates that it be running in FAIL mode. The reason for this is because this is the mode that actually enforces the TOE's DAC (and MAC, if configured) policy. If the TOE is not running in FAIL mode, the User Data Protection requirements cannot be enforced.

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 Top Secret components:

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

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 Top Secret is sufficient to ensure that these OS requirements were met.

Requirement	Description
Operating System	z/OS V1R9 or later OR The Customized Offerings Driver V3
A TSO/E Session	A TSO/E Session on the IPLed system must be established using a locally-attached or network-attached terminal
Proper Authority	Use the RACFDRV installation job as a sample of the security system definitions required so that a user can perform the installation tasks
Proper Security	In order to install the z/OS UNIX files, the following is required: • The ACID must be a superuser (UID=0) or have read access to the BPX.SUPERUSER resource in the RACF FACILITY class. • The ACID 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.
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. In addition, 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 should 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 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 should 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. • 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. However, IBM cannot directly recommend or endorse any specific application. 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. o 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 Top Secret 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 Top Secret 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 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with CA Top Secret for z/OS r14 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 Top Secret for z/OS r14 and are therefore not included in the TOE boundary.

- **ELM Integration** - Enterprise Log Manager is a separate product that collects and stores logs from various endpoints using agents configured with connectors.
- **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 is an independent product that requires its own license and is not included in the evaluated configuration of the TOE.

- **CA Top Secret® for DB2 –** Protects several DB2 resources and replaces GRANT/REVOKE processing. PERMIT commands are written in place of GRANT commands and a conversion utility provides a transition. A catalog synchronization utility brings DB2 catalog entries up-to-date with CA Top Secret for DB2 authorizations.
- **DFSMS** – IBM Subsystem. With DFSMS, the z/OS administrator can define performance goals and data availability requirements, create model data definitions for typical data sets, and automate data backup. DFSMS can automatically assign, based on installation policy, those services and data definition attributes to data sets when they are created.
- **Event Notification Facility (ENF)** - An operating system interface component CA Top Secret uses to obtain data from z/OS. CAIENF provides the VTAM facilities to transmit and receive TSS commands when using the Command Propagation Facility.
- **Standard Security Facility (SSF)** - A facility that provides an application interface for CA and non-CA products to obtain and use CA Top Secret information.

6.3.2 Installed but Requires a Separate License

There are no components that are installed with CA Top Secret for z/OS r14 that require a separate license.

6.3.3 Installed But Not Part of the TSF

These components are installed with CA Top Secret for z/OS r14, but are not included in the TSF.

- **Group** – Group is not commonly used. The intent is for its use is for backward compatibility. It is not used for object access.
- **User Attribute Data Set (UADS)** – In TSO, UADS is a partitioned data set with a member for each authorized user. Each member contains the appropriate passwords, user definitions, account numbers, LOGON procedure names, and user characteristics that define the user profile. This is an obsolete capability.
- **SYSPLEX** – The coupling facility is a feature of MVS/ESA 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.

- **CA Top Secret Workstation –** Provides:
  - A GUI for single-point administration of all CA Top Secret z/OS systems
  - Centralized monitoring and reporting of security events

- Security Modes – The following security modes are not security enforcing and are therefore not included in the evaluated configuration:
  - Dormant Mode - Although CA Top Secret is installed, it is not actively validating access. Checks are made for Administrators, but not for users.
  - Warn Mode – Warn mode is used to:
    - Determine which users are accessing which resources
    - Test the access definitions made in DORMANT mode

Warn mode can be set by facility, profile, user, resource, or event.

Note: Some applications make RACROUTE calls with the LOG=NOFAIL parameter. In WARN mode, these types of calls are written to the audit file if the check fails, but no message displays.

- Signon Violations - In WARN mode, define all users to CA Top Secret or CA Top Secret generates and records signon violations. WARN mode does not prevent an undefined user from signing on or gaining access to a protected resource.
- Password Violations - WARN mode does not prevent a defined user from signing on with an incorrect password, but this action generates a password violation.

Note: To force a defined user to supply a correct password in WARN mode, the WARNPW sub-option of the FACILITY control option must be set. Administrators must always supply a correct password, even in DORMANT mode.

- Resource Violations - If default protection is given to specific resource classes by attaching the DEFPROT attribute, WARN mode generates violations for all defined resources.
- Global Warn Mode - Use Global WARN mode to test segments of the implementation, or to back off from FAIL mode when an implemented segment of the organization is in trouble.

- **CA Mainframe Software Manager (MSM)** – The CA MSM is a utility used by the TOE that allows for the initial acquisition of CA Top Secret. 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.

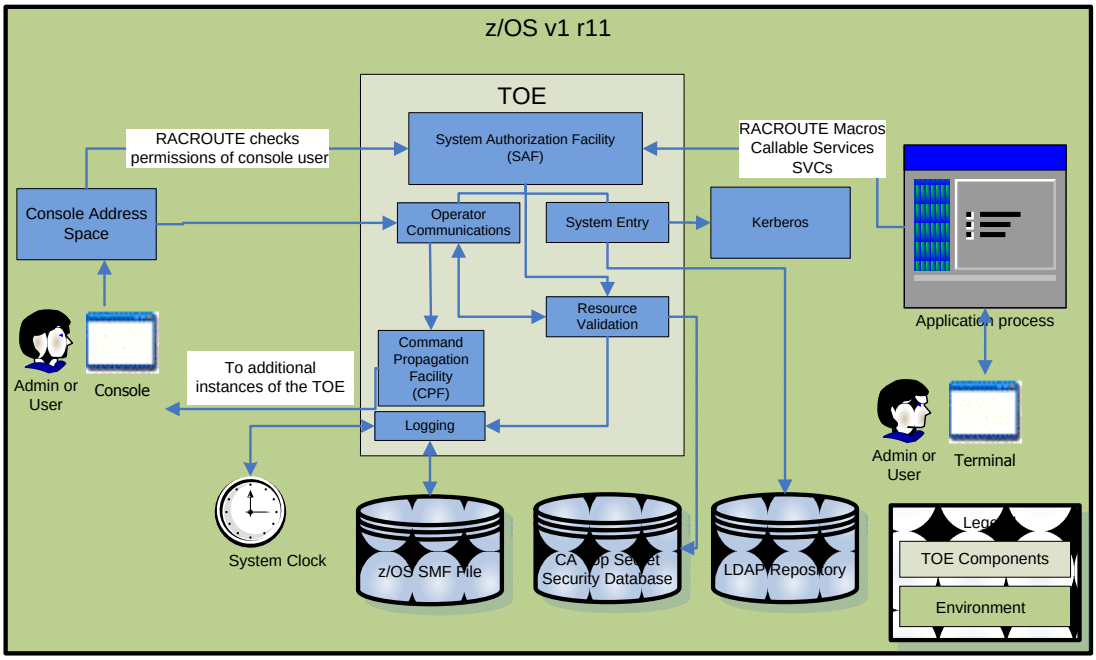

Figure 1 – TOE Boundary for CA Top Secret r14 SP1

8 TOE Acquisition

The NIAP-certified Top Secret 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 and were reviewed as part of the evaluation:

- CA Top Secret for z/OS Auditor Guide

- CA Top Secret for z/OS Best Practices Guide
- CA Top Secret for z/OS Command Functions Guide
- CA Top Secret for z/OS Compliance Information Analysis Guide
- CA Top Secret for z/OS Control Options Guide
- CA Top Secret for z/OS Cookbook
- CA Top Secret for z/OS Design Guide
- CA Top Secret for z/OS Implementation: CICS Guide
- CA Top Secret for z/OS Implementation: Other Interfaces Guide
- CA Top Secret for z/OS Installation Guide
- CA Top Secret for z/OS Message Reference Guide
- CA Top Secret for z/OS Multilevel Security Planning Guide
- CA Top Secret for z/OS Release Notes
- CA Top Secret for z/OS Report and Tracking Guide
- CA Top Secret for z/OS Troubleshooting Guide
- CA Top Secret for z/OS User Guide

9 IT Product Testing

The test team's test approach is to test the security mechanisms of CA Top Secret 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 Top Secret is processing the CPF updates. The greater vulnerability is in the z/OS (VTAM) storage, which is not under the direct control of Top Secret. 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 Top Secret command processor (TSS) is open in a user session to perform password changes, then the storage used by the TSS 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 TSS command terminates. If a system dump is taken of the user's address space while the command processor is open, the user passwords will be available in the storage used by the TSS 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 Top Secret r14 SP1 TOE meets the security requirements contained in the Security Target.

The criteria against which the Top Secret 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 Top Secret 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 Top Secret® r14 SP1 for z/OS Security Target, Version 1.1, March 7, 2011.

13 List of Acronyms

Acronym	Definition
ACID	Accessor ID
APPC	Advanced Program-to-Program Communication
ATF	Audit Tracking File
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme

CCIMB	Common Criteria Interpretations Management Board
CICS	Customer Information Control System
CNF	Certificate Name Filtering
CPF	Command Propagation Facility
DAC	Discretionary Access Control
DCA	Departmental Control ACID
DLF	Data Lookaside Table
EAL	Evaluation Assurance Level
FDT	Field Description Table
ICSF	Integrated Cryptographic Services Facility
IMS	Information Management System
JCL	Job Control List
LCF	Limited Command Facility
LSCA	Limit Central Security Control ACID
MAC	Mandatory Access Control
MLS	Multi-level Security
MSCA	Master Security Control ACID
MSM	Mainframe Software Manager
MVS	Multiple Virtual Storage
NDT	Node Description Table
PPT	Program Properties Table
RACF	Resource Access Control Facility
RDT	Resource Descriptor Table
SAF	System Authorization Facility
SCA	Central Security Control ACID
SDT	Static Data Table
SMF	System Management Facility
ST	Security Target
STC	Started Task Command
SYSID	System Identifier
TMP	Terminal Monitor Program
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSO	Time-sharing option
UADS	User Attribute Data Set
VCA	Divisional Control ACID
VSAM	Virtual Storage Access Method
ZCA	Zonal Control ACID

14 Terminology

Terminology	Definition
Access	Access indicates an ACID's ability to use a resource.
ACID	An ACID is a unique character-string identifier by which CA Top Secret identifies a user's Security Record.
ACID Authorities	ACID Authorities specify what actions security administrators can perform on ACIDs within their scope.
ACID Type	An ACID type determines an ACID's function in the Security File structure. Types include User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, and MSCA.
Administrator	An administrator is a user with privileges to manage the TOE, TOE data,

	and other TOE users. This includes security administrators and scoped security administrators. It can also include individual users that have been assigned the admin privilege.
Administrative authority	Administrative authority indicates the different classes of authority that are assigned via the TSS ADMIN command function. This field determines the functions a security administrator can perform.
ALL Record	The ALL Record contains global access requirements that are effective for all users.
Attribute	An attribute is a specific authority, privilege, or restriction that is assigned to an ACID.
Auditor	An authorized user or administrator with the audit privilege.
Authorization	Authorization is how CA Top Secret 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.
Central Security Control ACID	An SCA is an administrator whose scope of authority includes the entire installation. An SCA can designate and authorize VCAs and DCAs.
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 Top Secret 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.
Department	A department is a mandatory collection of users and profiles that a department ACID defines. A department cannot sign on and does not have a password, but it can own resources.
Department Control ACID	A Department Control ACID is used where security administration has been decentralized. The DCA's scope of authority is limited to the assigned department.
Division	A division is an optional collection of departments that a divisional ACID defines. A division cannot sign on and does not have a password, but it can own resources.
Divisional Control ACID	A VCA is an ACID used where security administration has been decentralized. The VCA's scope of authority is limited to an assigned division, including the departments attached to it.
Entity	An entity is the name of an object as referenced by the system and security.
Facility	A way of grouping options associated with a particular service that users sign on to.
Fail mode	FAIL mode indicates that CA Top Secret is in full control of all access requests. Violations result in termination of the request.
Field Description Table	The FDT contains all dynamically and pre-defined fields identified to CA Top Secret.
Global access	Global access indicates any access specified in the ALL Record.
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.
Information Management System	IBM Information Management System (IMS) is a joint hierarchical database and information management system with extensive transaction processing capabilities.
Job Control Language	The computer language that links a user's program to the computer, assigning files to specific devices and describing each file in detail to the system
Limited Central Security	LSCA is a control ACID can have all the authority of an SCA, but unlike

Control ACID	the SCA, the LSCA can have a limited scope of control. Only the MSCA can determine that scope and it can encompass ZCAs, VCAs, DCAs, Profiles, Users, and other LSCAs.
Limited Command Facility	LCF is a facility that allows the security administrator to control use of commands/transactions (TSO, CICS, and so on) available to a user.
Locktime	Locktime indicates the period of time after which a terminal automatically locks if no transactions or commands are issued. The user must issue TSS UNLOCK and supply a valid password to unlock the terminal.
Master Security Control ACID	MSCA is the one Control ACID that is predefined, active, and assigned full administrative authority the first time CA Top Secret starts. This administrator's scope of authority includes the entire installation. The MSCA can designate and authorize SCAs, LSCAs, ZCAs, VCAs, and DCAs.
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 Description Table	The NDT contains all PassTicket information.
Object	Any resource protected by the TOE.
Ownership	Ownership indicates when an ACID has unlimited access to the resource. Ownership defines the resource to CA Top Secret. All other ACIDs must be specifically authorized to access the resource.
Passphrase	A passphrase is a password that can be longer than eight characters and can contain blanks.
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 ACID, time of day, and session are needed.
Permissions	Permissions make an owned resource available to other users in a controlled manner.
Profile	A profile is an ACID containing a collection of access characteristics common to several users. It generally describes the access characteristics of a particular job function. A profile cannot sign on and does not have a password. Up to 254 profiles can be attached to a user's ACID. Any number of users can be associated with a single profile.
RACROUTE	The RACROUTE macro is the interface to RACF (or another external security manager) for z/OS.
Record	CA Top Secret supports several different record types. They include the main Security Record for each ACID, the Audit Record, the ALL Record, the Profile Record, the Department, Division, and Zone Records, the Resource Descriptor Table Record, and the Control ACID's Records.
Recovery File	The Recovery File contains a record of all changes made to the Security File. It is used to recreate the Security File if it becomes damaged or unusable because of hardware or software problems.
Resource	A resource is 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 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.
Resource Descriptor Table	The RDT contains all dynamically and pre-defined resources identified to CA Top Secret.
Scope of authority	Scope of authority indicates what logical units the user has administrative control over.
Secrec	See "Security Record."
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	A Security File is a Security Database consisting of the Security Records that contain all user and resource permissions and restrictions.
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 record (secrec)	A Security Record is part of the Security File that contains a set of user and profile records copied into a user's address space, including information such as resources a particular user can access and how the user can use them. This information also contains user characteristics, authorities, and so on. Also known as "secrec."
Security validation algorithm	The Security Validation Algorithm determines whether CA Top Secret should accept or deny users' requests to use a resource such as a data set.
Source of origin	Source or origin indicates the location of an access request (a terminal or reader).
Started Task Command Record	The Started Task Command (STC) Record is a reserved or special ACID that defines a z/OS started task command to CA Top Secret.
System Identifier	SYSID: A maximum of four characters may be specified and the value may contain an asterisk (*) for masking. This keyword is used along with certificate name filtering (CNF).
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	A user is the lowest ACID level in the security structure. Generally, a user can sign on via a password, initiate jobs, and belong to a department.
User Attribute Data Set	In TSO, UADS is a partitioned data set with a member for each authorized user. Each member contains the appropriate passwords, user definitions, account numbers, LOGON procedure names, and user characteristics that define the user profile.
Violation	A violation is an unauthorized attempt to access a protected resource.
Zone	A zone is an optional collection of divisions defined by a zone ACID. It cannot sign on and does not have a password, but it can own resources.
Zone Control ACID	A ZCA is an administrative ACID whose scope of authority includes an entire zone.