National Information Assurance Partnership

™

Common Criteria Evaluation and Validation Scheme Validation Report

CA Top Secret r15

Report Number: CCEVS-VR-VID10735-2016
Dated: June 2, 2016
Version: Version 1.0

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

ACKNOWLEDGEMENTS

Validation Team

Jean Petty
The MITRE Corporation

Daniel Faigin
Marybeth Panock
The Aerospace Corporation

Common Criteria Testing Laboratory

Christopher Gugel – CC Technical Director
Ronald Ausman
David Cornwell
Paul Juhasz
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

Table of Contents

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of CA Top Secret, provided by CA Technologies, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Linthicum Heights, Maryland, United States of America, and was completed in May 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Enterprise Security Management Access Control Protection Profile (ACPP) and Enterprise Security Management Policy Management Protection Profile (PMPP).

The Target of Evaluation (TOE) is CA Top Secret version r15. CA Top Secret is a mainframe software access control product that includes a policy management capability for administering access control policy enforcement. The TOE applies host-based access control rules to protect objects that reside on a z/OS mainframe system and define the permissions that individual users have to interact with the system.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the ACPP and PMPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the ACPP and PMPP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

The technical information included in this report was obtained from the CA Top Secret Security Target, Version 1.0, March 8, 2016 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities that are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profiles to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	CA Top Secret r15
Protection Profile	Standard Protection Profile for Enterprise Security Management Access Control v2.1 Standard Protection Profile for Enterprise Security Management Access Control v2.1
Security Target	CA Top Secret r15 Security Target, Version 1.0, March 8, 2016
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "CA Top Secret r15" Evaluation Technical Report v1.0 March 8, 2016
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

Sponsor	CA Technologies, Inc.
Developer	Booz Allen Hamilton, Linthicum, Maryland
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Linthicum, Maryland
CCEVS Validators	Jean Petty, MITRE Corporation Daniel Faigin, The Aerospace Corporation Marybeth Panock, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- The TOE will be capable of receiving access control policy data from its Operational Environment. Note that since the TOE claims both access control and policy management functionality, access control policy data may originate from within the TSF.
- The TOE will receive identity data from the Operational Environment.
- There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- The TOE will receive reliable time data from the Operational Environment.

3.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Basic.

- T.ADMIN_ERROR (from PMPP) – An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.

- T.CONTRADICT (from PMPP) – A careless administrator may create a policy that contains contradictory rules for access control enforcement.
- T.DISABLE (from ACPP) – 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.
- T.EAVES (from ACPP and PMPP) – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
- T.FALSIFY (from ACPP) – A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
- T.FORGE (from ACPP) – A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
- T.FORGE (from PMPP) – 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.
- T.MASK (from ACPP and PMPP) – A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
- T.NOROUTE (from ACPP) – A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
- T.OFLOWS (from ACPP) – A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior.
- T.UNAUTH (from ACPP) – 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.
- T.UNAUTH (from PMPP) – A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
- T.WEAKIA (from PMPP) – A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
- T.WEAKPOL (from PMPP) – 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.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- O.ACCESSID (from PMPP) – The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.
- O.AUDIT (from PMPP) – The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
- O.AUTH (from PMPP) – 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.
- O.CONSISTENT (from PMPP) – The TSF will provide a mechanism to identify and rectify contradictory policy data.
- O.DATAPROT (from ACPP) – The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
- O.DISTRIB (from PMPP) – The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
- O.INTEGRITY (from ACPP) – The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.
- O.INTEGRITY (from PMPP) – The TOE will contain the ability to assert the integrity of policy data.
- O.MAINTAIN (from ACPP) – The TOE will be capable of maintaining policy enforcement if disconnected from the Policy Management product.
- O.MANAGE – The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
- O.MNGRID (from ACPP) – The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.
- O.MONITOR (from ACPP) – 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).

- O.OFLOWS (from ACPP) – The TOE will be able to recognize and discard invalid or malicious input provided by users.
- O.POLICY (from PMPP) – 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.
- O.PROTCOMMS (from ACPP and PMPP) – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
- O.ROBUST (from PMPP) – The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
- O.SELFID (from ACPP) – The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.
- O.SELFID (from PMPP) – The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

3.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Standard Protection Profile for Enterprise Security Management Access Control v2.1, 24 October 2013 and Standard Protection Profile for Enterprise Security Management Policy Management v2.1, 24 October 2013 to which this evaluation claimed exact compliance.
- Consistent with the expectations of the Protection Profiles, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Section 6 of the Security Target and their operation with respect to the TOE is described in Section 8 of the Security Target. Any

other functions provided by CA Top Secret needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated configuration of the TOE is the CA Top Secret software product. The TOE includes all the code that enforces the policies identified (see Section 5).

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

CA Top Secret (also referred to as the TOE) is host-based access control product for z/OS mainframe systems. It interacts with the IBM System Authorization Facility (SAF) to evaluate operations being attempted against the mainframe system and applies access control policy rules to the request in order to determine if the requested operations should be permitted. It provides its own policy management capability to allow administrators to define access control rules to be enforced on the system. Through the use of the Command Propagation Facility (CPF), multiple distinct LPARs/systems can be administered simultaneously through the ability of an administrator to use Top Secret to issue commands to remote instances of the product.

4.2 Physical Boundary

The physical boundary of the TOE includes the CA Top Secret software that is installed on top of the z/OS operating 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 that is required for the TOE to run. The following table lists the software components that are required for the TOE's use in the evaluated configuration. These Operational Environment components are expected to be patched to include the latest security fixes for each component.

Component	Requirement
Platform	IBM System z mainframe (zEC12, z114, z196, z9 series, z10 series)
System Components	• INIT/JOB • JES2 • TSO • TCP/IP • VTAM • CA Common Services for z/OS r11 SP6 or above • CA LDAP Server for z/OS r15 • IBM Integrated Cryptographic Module Facility (ICSF) • IBM System SSL • IBM Ported Tools for z/OS – OpenSSH

In addition to the mainframe requirements, a TN3270e terminal emulator is required for any system used to administer the TOE via TSO or JES2. In the evaluated configuration, the TOE was tested using QWS3270 over an SSH tunnel that was established using the CA Common Services, ICSF, and OpenSSH environmental components.

5 Security Policy

5.1 Enterprise Security Management

CA Top Secret provides enterprise security management through its ability to define and enforce access control policies. The TOE provides the ability to define these policies through a command line interface. Policies can be defined to control access to processes, files, system configuration, and use of the authentication function for mainframe systems. The TOE also defines subject attributes for mainframe users that can affect how access control policies are audited for specific users. Since the TOE can enforce access control against the mainframe's authentication function, it ensures that all users and administrators are identified and authenticated prior to accessing any objects that reside on the system, including the TSF itself.

5.2 Security Audit

The TOE generates audit records of its behavior and administrator activities. Audit data includes date, time, event type, subject identity, and other data as required. Audit data is written to the mainframe's SYSLOG and SMF audit storage repositories in the Operational Environment. The administrator has some degree of control over the types of events that are audited for access control functionality in order to minimize the volume of audit data.

5.3 Communications

The TOE can communicate policy rules to remote instances of Top Secret that are located on distributed systems or LPARs using the Command Propagation Facility (CPF). CPF provides transaction receipts to administrators so that the implementation status of transmitted policy rules can be determined. If a remote node is unavailable to receive CPF commands, they will be queued and transmission will be periodically retried until the node is available.

5.4 User Data Protection

The TOE has the ability to enforce access control against files, processes, system configuration objects, and the authentication function of a mainframe system. Access control policy rules can be written against arbitrarily-defined subjects and objects so that anything that resides on the system can be protected as needed. The TSF implements a rule sorting algorithm in order to give better matched rules higher priority which prevents rules from coming into conflict with one another. The TSF also defines several exceptions to the rule enforcement engine so that specific overrides can be granted if

necessary. By default, the TOE considers the system objects that comprise itself to be protected so that an untrusted user is unable to bypass, terminate, or control the behavior of the access control enforcement mechanism.

5.5 Identification and Authentication

The TOE provides mechanisms to minimize the likelihood of a successful brute force attack against the mainframe's authentication function. Specifically, the TSF can suspend a user account after it has exceeded a configurable number of failed authentication attempts and is locked out until and unlocked by an administrator. Subject attributes are associated with users based on the user's definition in the mainframe's internal user database regardless of whether that user is defined by manual administrative commands or by the environmental LDAP server translating LDAP queries into actions that configure the mainframe user database.

5.6 Security Management

The TOE is managed by authorized administrators using CLI commands. CLI commands can be issued in batch jobs or interactively using TSO. The TSF provides the ability to manage the TOE's functionality as well as the access control policies that are enforced by the TSF, both on the local system and on remote nodes using CPF. There are several distinct administrative roles with differing levels of privilege to interact with the TSF.

5.7 Protection of the TSF

The TOE does not provide a mechanism to view administrator credential data and does not store any key data. The TOE is able to use the Common Services and ICSF environmental components to encrypt CPF commands sent to remote nodes, preventing replay attacks against transmitted policy data. In a CPF environment, the loss of communications between distributed nodes does not affect the TOE's ability to enforce the access control policy rules that it has consumed.

5.8 Resource Utilization

In a CPF environment, the TOE will queue CPF commands that fail to reach a remote node during a period of communications outage and will periodically attempt to transmit them so that up-to-date configuration of the TSF can be performed automatically once communications are restored.

5.9 TOE Access

The TOE's access control enforcement mechanism can deny session establishment to users and administrators based on policy rules such as day, time, and the method used to access the mainframe system.

5.10 Trusted Path/Channels

The TOE does not provide its own cryptography. In the evaluated configuration, CA Common Services is used to provide TCP/IP configurations between the TOE and remote entities and the following components are used to establish trusted communications:

- ICSF and System SSL to secure TLS communications
- IBM Ported Tools for z/OS – OpenSSH and ICSF to secure SSH communications

The TSF is able to rely on the Operational Environment to secure remote CPF commands using TLS and remote administrative sessions using SSH.

6 Documentation

The vendor provides a standard set of guidance documents that covers the core functionality of the product. These documents were used during the evaluation of the TOE:

- Audit Guide, CA Top Secret for z/OS r15
- Best Practices Guide, CA Top Secret for z/OS r15
- Installation Guide, CA Top Secret for z/OS r15
- Quick Reference Guide, CA Top Secret for z/OS r15
- User Guide, CA Top Secret for z/OS r15
- Control Options Guide, CA Top Secret for z/OS r15
- Report and Tracking Guide, CA Top Secret for z/OS r15
- CA Top Secret r15 Supplemental Administrative Guidance for Common Criteria

These guidance documents contain the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance documents are applicable for the version of CA Top Secret claimed by this evaluation.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the CA Top Secret software installed on IBM z/OS.

To use the product in the evaluated configuration, the product must be configured as specified in the CA Top Secret r15 Supplemental Administrative Guidance for Common Criteria document. Refer to Section 6 for the full list of documents needed for instructions on how to place the TOE in its evaluated configuration.

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Evaluation Technical Report for a Target of Evaluation "CA Top Secret r15" Evaluation Technical Report v1.0 dated March 8, 2016*, which is not publically available.

8.1 Test Configuration

Testing was executed at the vendor site in Ewing, NJ by connecting physically to the test systems via direct line to prevent disclosure or modification of data in transit. This connection was logically secured using SSH in order to demonstrate that the TSF is capable of satisfying FTP_TRP.1. Booz Allen reviewed the physical security controls of the test environment and interviewed CA employees to ensure that the testing environment was not subject to unauthorized tampering.

The evaluation team installed and configured the TOE according to the CA Top Secret r15 Supplemental Administrative Guidance for Common Criteria document for testing.

The following environment components and test tools* were utilized during the testing:

- IBM z/OS 2.1
- CA Chorus Software Manager
- CA LDAP Server r15.1
- CA Common Services r14
- CA WebAdmin r15
- TCP/IP v4.0 for IBM z/OS
- IBM Integrated Cryptographic Services Facility (ICSF)
- IBM System SSL
- IBM Ported Tools for z/OS – OpenSSH
- JES2 v2.1
- TSO v4.1
- CICS r5.1
- QWS3270

* Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.3 Evaluation Team Independent Testing

The functional testing was conducted during December 2015 at the vendor site in Ewing, NJ. The only way to access the test environment was from a CA-owned laptop that was connected to the test network. Any configuration performed by CA personnel during the functional testing timeframe was conducted using the AGD as guidance and under the supervision of the evaluators.

The test team's approach was to test the security mechanisms of the CA Top Secret software by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface was described in the relevant design documentation (e.g., ST and AGD) in terms of the claims on the TOE that can be tested through the external interface. The "CA Top Secret r15 Security Target v1.0" (ST), "CA Top Secret Supplemental Administrative Guidance for Common Criteria v1.0" (AGD), the "CA Top Secret ATE Test Matrix Results" (Test Matrix), and "CA Top Secret Test Procedures" (Test Plan) were used to demonstrate test coverage of all SFR testing assurance activities as defined by the ACPP and PMPP for all security relevant TOE external interfaces. TOE external interfaces that were determined to be security relevant are interfaces that do any of the following:

- 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
- Invoke or configure a security mechanism.

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

In order to determine that the TSF sufficiently addressed the requirements for host-based access control as defined by ACPP, the evaluators identified the z/OS system objects that represented the objects defined in ACPP (programs, files, host configuration, and authentication function). The evaluators then identified types of access control policy rules that Top Secret can define in order to control access to these objects. These policy rules were considered to be within the scope of the TOE. The evaluators then tested these rules by demonstrating the ability of mainframe users and started tasks to access (or not access) arbitrarily chosen examples of the tested system objects based on access control rules written against these objects.

8.4 Evaluation Team Vulnerability Testing

The vulnerability analysis is in a proprietary report prepared by the lab. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerabilities.

The vulnerability search did not yield any readily apparent security flaws in the TOE or any of the major z/OS components that it interfaces with; however, the search process allowed the evaluators to focus on 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:

- *Escalation of Privileges* – the evaluators attempted to escalate their own privileges as defined by the TSF by attempting to modify the in-storage access rules in memory and by attempting to circumvent the access control SFP by taking valid privileges to modify a system object and passing them to a program that uses those privileges to gain unauthorized access to a different object.
- *Virtual Storage Access Method (VSAM) IDCAMS Utility* – the evaluators used the IDCAMS utility to attempt to dump raw data from the Top Secret databases into a flat file in order to see if any TSF data is disclosed without authorization.
- *Auditing SMF Records* – the evaluators reviewed raw unformatted dumps of audit data to search their contents for data that could be used to gain unauthorized access to the TOE or to the underlying system protected by the TSF.
- *System Penetration* – the evaluators performed several small miscellaneous tests that did not pertain to specific categories that collectively attempted to circumvent the TOE's access control enforcement mechanisms.
    - Use of AMASPZAP service aid to attempt to dynamically dump program data to see if a program's runtime execution can be modified in a way that could potentially bypass access control checking.
    - Attempt to issue a console command using a batch job to determine what privileges are applied to the request. If a user is not authorized to issue console commands, attempting to do so through an intermediary may bypass access control checking.
    - Attempt to issue protected console commands with both privileged and non-privileged user accounts as well as attempt to issue a command to the TSF from the console. Use of the console interface could potentially grant additional authorizations above and beyond what is granted to the user.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Assurance Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4, and the assurance activities defined in the Protection Profiles with which the ST claimed conformance. The evaluation determined the CA Top Secret TOE to be Part 2 extended and meet the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the ACPP and PMPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the ACPP and PMPP.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit specified in the ACPP and PMPP (the work units are identical between the two). The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification as well as a separately developed Functional Specification document.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities as defined by the

CEM and specified in the ACPP and the PMPP, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit specified in the ACPP and PMPP (the work units are identical between the two). The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities as defined by the CEM and specified in the ACPP and PMPP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit specified in the ACPP and PMPP (the work units are identical between the two), as well as the Assurance Activities specified for ALC_CMC.1 and ALC_CMS.1. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit specified in the ACPP and PMPP (the work units are identical between the two). The evaluation team ran the set of tests specified by the Assurance Activities defined by the CEM and specified in the ACPP and PMPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the ACPP and PMPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit specified in the ACPP and PMPP (the work units are identical between the two). The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the ACPP and PMPP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities as defined by the CEM and specified in the ACPP and PMPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team has the following additional comments about this validation:

1. The evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the CA Top Secret Supplemental Administrative Guidance for Common Criteria.

2. That the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.
   The evaluation laboratory performed an extensive amount of testing for the ability of the product to enforce password composition rules. It was determined that while the majority of password policy requirements were implemented by the product, it does not allow an administrator to define the minimum number of characters that must be changed when updating password phrase credentials. Therefore, the optional requirement FIA_SOS.1 was omitted from the ST.

3. The audit data that is generated by the TOE is formatted as mainframe SYSLOG and SMF data. This audit data is machine-readable and is typically converted to a human-readable format by third-party utilities. Customers are cautioned that familiarity with the mainframe log formats is recommended in order to decipher the audit trail data.

4. Understanding and working with this product, including the ability to validate the test evidence, requires familiarity with mainframe language/syntax, processes and procedures. Support from Subject Matter Experts may be required.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *CA Top Secret r15 Security Target, Version 1.0, March 8, 2016.*

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

13 List of Acronyms

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

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

VCA	Division Control Administrator
ZCA	Zone Control Administrator

14 Terminology

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

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.

	interact with mainframe resources and Top Secret is adjudicating their actions against its access control policy.
User ACID	A type of ACID used to define user accounts.
Zone	An arbitrary organizational unit defined by the TSF that contains two or more divisions.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. CA Top Secret r15 Security Target, Version 1.0, March 8, 2016.
6. Evaluation Technical Report for a Target of Evaluation "CA Top Secret r15" Evaluation Technical Report v1.0 dated March 8, 2016.
7. CA Top Secret r15 Supplemental Administrative Guidance for Common Criteria
8. CA Top Secret Common Criteria Evaluation Test Plan (Test Procedures)
9. Vulnerability Analysis CA Top Secret r15
10. Audit Guide, CA Top Secret for z/OS r15
11. Best Practices Guide, CA Top Secret for z/OS r15
12. Installation Guide, CA Top Secret for z/OS r15
13. Quick Reference Guide, CA Top Secret for z/OS r15
14. User Guide, CA Top Secret for z/OS r15
15. Control Options Guide, CA Top Secret for z/OS r15
16. Report and Tracking Guide, CA Top Secret for z/OS r15

Note: The phrase "Top Secret" used in this document refers to a product from CA, and is not a security label marking.