National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Standard Protection Profile for Enterprise Security Management Access Control, Version 2.1, October 24th, 2013

Report Number: CCEVS-VR-PP-0009
Dated: 31 July 2015
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

Common Criteria Testing Laboratory

Base Requirements
Computer Sciences Corporation
Hanover, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Standard Protection Profile for Enterprise Security Management Access Control, Version 2.1 (ESMACPP21). It presents a summary of the ESMACPP21 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the ESMACPP21 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the CA Layer 7 SecureSpan SOA Gateway, version 8.0. The evaluation was performed by the Computer Sciences Corporation (CSC) Common Criteria Testing Laboratory (CCTL) in Hanover, Maryland, United States of America, and was completed in May 2014. This evaluation addressed the base requirements of the ESMACPP.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the CSC CCTL.

The evaluation determined that the ESMACPP21 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP 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). The ST contains material drawn directly from the ESMACPP21 as well as the Standard Protection Profile for Enterprise Security Management Policy Management. Performance of the majority of the ASE work units serves to satisfy the APE work units as well for both of these claimed PPs. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the ESMACPP21 meets the requirements of the APE components. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the ESMACPP21 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the CA Layer 7 SecureSpan SOA Gateway, Version 8.0, developed by CA, Inc. The evaluation was performed by the Computer Sciences Corporation Common

Criteria Testing Laboratory (CCTL) in Hanover, Maryland, United States of America, and was completed in May 2014.

The ESMACPP21 contains a set of "base" requirements that all conformant STs must include and "additional" requirements that may or may not apply to a conformant TOE depending on its architecture and intended usage.

Because these optional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the ESMACPP21 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the ESMACPP21.

Protection Profile	*Standard Protection Profile for Enterprise Security Management Access Control, Version 2.1*
ST (Base)	CA Layer 7 SecureSpan SOA Gateway v8.0 Security Target, May 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (base)	Computer Sciences Corporation, Hanover, MD USA
CCEVS Validators (base)	Daniel Faigin, Aerospace Corporation Jerome Myers, Aerospace Corporation

3 ESMACPP Description

This Protection Profile focuses on access control decision and enforcement. A product/product component that conforms to this Protection Profile consumes a centrally-defined access control policy and enforces it. In doing so, it provides preventative security to the enterprise in a consistent manner. A product that conforms to this Protection Profile is expected to intercept requests against some type of defined resource (such as a file system object on a workstation or a web site on an organizational intranet) and determine if the request should be allowed. In an ESM environment, this capability is called a Policy Decision Point, or PDP. It will then enforce the results of this determination or pass the decision to a trusted entity that does the enforcement itself. In an ESM environment, this second capability is called a Policy Enforcement Point, or PEP. Products that are compliant with the profile defined in this document provide both Policy Decision and Policy Enforcement. Some ESM products only provide policy decision and defer enforcement to the operating environment; in such cases, the only way to evaluate such products against this Profile is to draw the TOE boundary such that the operational environment enforcement component is recategorized as a TOE component.
It is important to understand how ESM access control differs from the access control commonly found in an operating system:

- ESM Access Control is centrally provisioned: ESM Access Control enforces a centrally-defined policy, whereas an operating system enforces a locally-defined policy (i.e., a policy that is both local to and specific to that particular operating system). The ability to define a central access control policy and have it apply uniformly across the organization to a given set of users and/or IT assets allows for consistent application of organizational security policies.
- ESM Access Control operates on organizationally defined objects: ESM Access Control policies often operate on objects of different granularity than an operating system. Whereas an operating system focuses on fundamental objects such as files and IPC interfaces, an ESM product has the ability to operate on higher-level abstractions that may be implemented as a combination of fundamental objects (for example, an ―order‖, which might be a combination of multiple files). Thus ESM products provide the capability to mediate web transactions or prevent data exfiltration at a mail gateway. An ESM Access Control product that functions as an agent on an operating system will be deployed to perform a supplemental role to the native OS capabilities such as whitelisting applications that are created by trusted vendors (and more significantly, it can enforce a centrally-defined policy).
- ESM Access Control is based on organizational identities: ESM Access Control products operate using centralized identity data, as opposed to an operating system-specific user base. This permits access control to be configured using organizational attributes and contexts that the organization deems to be important instead of forcing policies to be broken down by legacy user and group distinctions.

A compliant TOE that claims conformance to this PP will be used to control access to local or network resources using a mechanism that is not innately provided by an operating system on which the resource resides. This includes products such as external security managers that supplement the access control mechanisms provided by a host and web content filters.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE. Note that depending on the architecture of the TOE, some aspects of the security problem may be addressed either by the TOE or by the Operational Environment. These items are designated as optional assumptions to refer to the fact that these behaviors have the potential to be addressed by the TOE.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.CRYPTO (optional)	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.INSTALL	There will be a competent and trusted administrator who will follow

Assumption Name	Assumption Definition
	the guidance provided in order to install the TOE.
A.POLICY	The TOE will receive policy data from the Operational Environment.
A.ROBUST (optional)	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME (optional)	The TOE will receive reliable time data from the Operational Environment.
A.USERID	The TOE will receive identity data from the Operational Environment.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.DISABLE	A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FALSIFY	A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
T.FORGE	A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.NOROUTE	A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
T.OFLOWS	A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior.
T.UNAUTH	A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.

4.3 Organizational Security Policies

Table 3: Threats

OSP Name	OSP Definition
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

4.4 Security Objectives

The following table contains security objectives for the TOE. Similar to the assumptions, since some threats may be addressed either by the TOE or by its underlying Operational Environment, some security objectives may apply to either. Objectives that can be assigned in this manner are labeled as optional as well as any objectives that are strictly optional because not all compliant TOEs will have an architecture that requires them to be present.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.CRYPTO (optional)	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
O.DATAPROT	The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
O.INTEGRITY	The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.
O.MAINTAIN	The TOE will be capable of maintaining access control policy enforcement if it is unable to communicate with the Policy Management product which provided it the policy.
O.MNGRID	The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.
O.MONITOR	The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users).
O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.RESILIENT (optional)	If the TOE mediates actions performed by a user against resources on an operating system, the system administrator or user shall not be allowed to perform an operation in the Operational Environment that would disable or otherwise modify the behavior of the TOE.
O.SELFID	The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.CRYPTO (optional)	The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.

Environmental Security Obj.	TOE Security Objective Definition
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.POLICY	The Operational Environment will provide a policy that the TOE will enforce.
OE.PROTECT (optional)	The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.
OE.USERID	The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.

5 Requirements

As indicated above, requirements in the ESMACPP21 are comprised of the "base" requirements and additional requirements that are conditionally or strictly optional. The following are table contains the "base" requirements that were validated as part of the CA evaluation activity referenced above.

Requirement Class	Requirement Component
ESM: Enterprise Security Management	ESM_EID.1: Reliance on Enterprise Identification
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SEL.1: Selective Audit
	FAU_STG.1 Protected Audit Trail Storage (Local Storage)
	FAU_STG_EXT.1: External Audit Trail Storage
FCO: Communications	FCS_NRR.2: Enforced Proof of Receipt
FDP: User Data Protection	FDP_ACC.1: Subset Access Control
	FDP_ACF.1: Security Attribute Based Access Control
FMT: Security Management	FMT_MOF.1(1): Management of Functions Behavior
	FMT_MOF.1(2): Management of Functions Behavior
	FMT_MSA.1: Management of Security Attributes
	FMT_MSA.3: Static Attribute Initialization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Stored Credentials
	FPT_FLS_EXT.1: Failure of Communications
	FPT_SKP_EXT.1: Protection of Secret Key Parameters
	FPT_RPL.1: Replay Detection
FRU: Resource Utilization	FRU_FLT.1: Degraded Fault Tolerance
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel

Also note that there are multiple instances of FDP_ACC.1 and FDP_ACF.1. The PP defines multiple allowable access control scenarios, one of which is expected to be claimed by a compliant TOE. These requirements were observed to be consistent with one another in all

respects except for assignment text that was completed by the PP author to appropriately describe each scenario.

The following table contains the optional requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
ESM: Enterprise Security Management	ESM_DSC.1: Object Discovery	
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	
	FCS_CKM_EXT.4: Cryptographic Key Zeroization	
	FCS_COP.1(1): Cryptographic Operation	
	FCS_COP.1(2): Cryptographic Operation	
	FCS_COP.1(3): Cryptographic Operation	
	FCS_COP.1(4): Cryptographic Operation	
	FCS_HTTPS_EXT.1: HTTPS	
	FCS_IPSEC_EXT.1: IPsec	
	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	
	FCS_SSH_EXT.1: SSH	
	FCS_TLS_EXT.1: TLS	
FPT: Protection of the TSF	FPT_FLS.1: Failure with Preservation of a Secure State	
FTA: TOE Access	FTA_TSE.1: TOE Session Establishment	

6 Assurance Requirements

The following are the assurance requirements contained in the ESMACPP21:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Pass

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the ESMACPP Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Computer Sciences Corporation, *CA Layer 7 SecureSpan SOA Gateway v8.0 Security Target*, Version Unspecified. May, 2014.

[7] Standard Protection Profile for Enterprise Security Management Access Control, Version 2.1, October 24, 2013.