National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Standard Protection Profile for Enterprise Security Management and Credential Management, Version 2.1, October 24th, 2013

Report Number:	**CCEVS-VR-PP-0018**
Dated:	**28 October 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 and Additional Requirements
Booz Allen Hamilton.
Linthicum, 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 Identity and Credential Management, Version 2.1 (ESMICMPP21). It presents a summary of the ESMICMPP21 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the ESMICMPP21 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 Oracle Identity Manager (OIM) 11g Release 2. The evaluation was performed by the Booz Allen Hamilton. Common Criteria Testing Laboratory (CCTL) in Linthicum, Maryland, United States of America, and was completed in August 2015. This evaluation addressed the base requirements of the ESMICMPP21, as well as a few of the additional requirements contained in Appendix C.

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

The evaluation determined that the ESMICMPP21 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). Because the ST contains only material drawn directly from the ESMICMPP21, performance of the majority of the ASE work units serves to satisfy the APE work units as well. 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 ESMICMPP21 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the evaluation technical 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 ESMICMPP21 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Oracle Identity Manager (OIM), provided by Oracle Corporation. The evaluation was performed by the Booz Allen Hamilton. Common Criteria Testing

Laboratory (CCTL) in Linthicum, Maryland, United States of America, and was completed in August 2015.

The ESMICMPP21 contains a set of “base” requirements that all conformant STs must include as well as “additional” requirements that are either conditional or strictly optional, depending on the requirement in question. The vendor may choose to include such requirements in the ST and still claim conformance to this PP. If the vendor’s TOE performs capabilities that are governed by any additional requirements, that vendor is expected to claim all of the additional requirements that relate to these capabilities.

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 ESMICMPP21 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 ESMICMPP21.

Protection Profile	*Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1, October 24, 2013*
ST (Base)	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
ST (Additional)	SailPoint IdentityIQ Common Criteria Security Target, Version 1.0, September 16, 2015
Evaluation Technical Report (Base)	Evaluation Technical Report for Oracle Identity Manager, Version 11g Release 2, August 13, 2015
Evaluation Technical Report (Additional)	Evaluation Technical Report for SailPoint IdentityIQ Version 1.0, August 19, 2015
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 and additional)	Booz Allen Hamilton, Linthicum, MD USA
CCEVS Validators (base)	Daniel Faigin, Aerospace Corporation Dr. Patrick Mallett, MITRE Corporation Jean Petty, MITRE Corporation
CCEVS Validators (Additional)	Daniel Faigin, Aerospace Corporation Meredith Hennan, Aerospace Corporation

3 ESMICMPP Description

This protection profile focuses on the aspect of ESM that is responsible for enforcing identity and credential management. Identity and Credential Management products will generate and issue credentials for subjects that reside within the enterprise. They will also maintain the organizational attributes that are associated with these subjects. By providing a means for subjects to validate their identities and determining the relationship these subjects have to the enterprise, an Identity and Credential Management product is able to support enterprise accountability and access control.

The establishment of unique, unambiguous identities is an important foundational capability that enables issuance and management of credentials and authorization attributes. The notion of identity refers to that unique identifier assigned to an individual against which credential and attribute data can be associated.

In order for an individual to be identified as a user within the ESM system, they must be enrolled. Enrollment refers to the act of assigning a unique identifier to a subject, generating and issuing credentials, defining attributes for a user, and propagating that data to any repositories that use it. It is necessary for the TSF to be able to securely transmit this data to those components.

TOEs compliant with this PP are expected to exhibit the following behavior:

- Provisioning of subjects (enroll new subjects to an organizational repository, associate and disassociate subjects with organizationally-defined attributes)
- Issue and maintain credentials associated with user identities
- Publish and change credential status (such as active, suspended, or terminated)
- Establish appropriate trusted channels between itself and compatible Policy Management and Authentication Server ESM products
- Generate an audit trail of configuration changes and subject identification and authentication activities
- Write audit trail data to a trusted repository
- Securely transmit identity and credential attribute data via a trusted channel

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.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.CRYPTO	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.ENROLLMENT	There will be a defined enrollment process that confirms user identity before the assignment of credentials
A.ROBUST	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate

Assumption Name	Assumption Definition
	user during authentication.
A.FEDERATE	Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data
T.FALSIFY	A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment.
T.FORGE	A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.
T. INSUFFATR	An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.RAWCRED	A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.
T.UNAUTH	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	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

4.3 Organizational Security Policies

Table 3: Organizational Security Policies

Threat Name	Threat Definition
P.BANNER	The TOE shall display an initial banner describing restrictions of use,

Threat Name	Threat Definition
	legal agreements, or any other appropriate information to which users consent by accessing the system.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.ACCESSID	The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users
O.AUTH	The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.CRYPTO	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
O.EXPORT	The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.
O.IDENT	The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.
O.INTEGRITY	The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.
O.MANAGE	The TOE will provide Assignment Managers with the capability to manage the TSF.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTCRED	The TOE will be able to protect stored credentials.
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

TOE Security Obj.	TOE Security Objective Definition
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject

TOE Security Obj.	TOE Security Objective Definition
	identity to attribute mappings within the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic mechanisms that are used to ensure the confidentiality and integrity of communications.
OE.ENROLLMENT	The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.
OE.FEDERATE	Data the TOE exchanges with trusted external entities is trusted.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.MANAGEMENT	The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE
OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.

5 Requirements

As indicated above, requirements in the ESMICMPP21 are comprised of the “base” requirements and additional requirements that are conditionally optional. The following are table contains the “base” requirements that were validated as part of the Oracle evaluation activity referenced above.

Requirement Class	Requirement Component
ESM: Enterprise Security Management	ESM_EAU.2: Reliance on Enterprise Authentication
	ESM_EID.2: Reliance on Enterprise Identification
	ESM_ICD.1: Identity and Credential Definition
	ESM_ICT.1: Identity and Credential Transmission
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Audit Association
	FAU_STG.1: Protected Audit Trail Storage (Local Storage)
	FAU_STG_EXT.1: External Audit Trail Storage
FIA: Identification and Authentication	FIA_USB.1: User-Subject Binding
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Management Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Stored Credentials
	FPT_SKP_EXT.1: Protection of Secret Key Parameters

Requirement Class	Requirement Component
FTA: TOE Access	FTA_TAB.1: TOE Access Banners
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path

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_ATD.1: Object Attribute Definition	
FAU: Security Audit	FAU_SEL.1:Selectable Audit	
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation (Asymmetric Keys)	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
	FCS_CKM_EXT.4: Cryptographic Key Zeroization	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
	FCS_COP.1(1): Cryptographic Operation (for Data Encryption/Decryption)	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
	FCS_COP.1(2): Cryptographic Operation (for Cryptographic Signature)	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
	FCS_COP.1(3): Cryptographic Operation (for Cryptographic Hashing)	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
	FCS_COP.1(4): Cryptographic Operation (for Keyed-Hash Message Authentication)	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
	FCS_IPSEC_EXT.1: IPsec	
	FCS_HTTPS_EXT.1: HTTPS	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
	FCS_SSH_EXT.1: Secure Shell	
	FCS_TLS_EXT.1: Transport Layer Security (TLS)	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling	SailPoint IdentityIQ Security Target, Version 1.0, September 16, 2015
	FIA_SOS.1: Verification of Secrets	SailPoint IdentityIQ Security Target, Version 1.0, September 16, 2015
FMT: Security Management	FMT_MTD.1: Management of TSF Data	Oracle Identity Manager Security Target, Version 1.0, July 29, 2015
FPT: Protection of the TSF	FPT_STM.1: Reliable Time Stamps	
FTA: TOE Access	FTA_SSL_EXT.1: TSF-initiated Session Locking	
	FTA_SSL.3:TSF-initiated Termination	SailPoint IdentityIQ Security Target, Version 1.0, September

Requirement Class	Requirement Component	Verified By
		16, 2015
	FTA_SSL.4: User-initiated Termination	SailPoint IdentityIQ Security Target, Version 1.0, September 16, 2015
	FTA_TSE.1: TOE Session Establishment	

6 Assurance Requirements

The following are the assurance requirements contained in the ESMICMPP21:

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 ESMICMPP 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] Booz Allen Hamilton *Oracle Identity Manager Security Target,* Version 1.0, July 29, 2015

[7] Booz Allen Hamilton *SailPoint IdentityIQ Security Target,* Version 1.0, September 16, 2015

[8] Booz Allen Hamilton *Evaluation Technical Report for Oracle Identity Manager*, Version 11g Release 2, August 13, 2015

[9] Booz Allen Hamilton *Evaluation Technical Report for SailPoint IdentityIQ*, August 19, 2015

[10] Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1, October 24, 2015