National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

RSA Identity Governance and Lifecycle v7.0.1

Report Number: CCEVS-VR-VID10769-2017
Dated: May 31, 2017
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

Table of Contents

1 Executive Summary 2
2 Identification 4
2.1 Threats 4
2.2 Organizational Security Policies 5
3 Architectural Information 6
4 Assumptions 7
4.1 Clarification of Scope 7
5 Security Policy 8
5.1 Enterprise Security Management 8
5.2 Security Audit 8
5.3 Identification and Authentication 8
5.4 Security Management 8
5.5 Protection of the TSF 8
5.6 TOE Access 8
5.7 Trusted Path/Channels 8
6 Documentation 10
7 Independent Testing 11
7.1 Penetration Testing 12
8 Evaluated Configuration 13
9 Results of the Evaluation 14
10 Validator Comments/Recommendations 15
11 Annexes 16
12 Security Target 17
13 Abbreviations and Acronyms 18
14 Bibliography 19

List of Tables

Table 1: Evaluation Details 3
Table 2: ST and TOE Identification 4
Table 3 TOE Security Assurance Requirements 14

List of Figures

Figure 1 TOE Boundary 6
Figure 2 Test Configuration 11

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Application Software in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the RSA Identity Governance and Lifecycle v7.0.1. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the RSA Identity Governance and Lifecycle v7.0.1 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in February 2017. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013, and including the following optional SFRs: FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, and FTA_TAB.1[1].

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the RSA Identity Governance and Lifecycle v7.0.1 is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) [8] and associated test report [7] produced by the Leidos evaluation team.

RSA Identity Governance and Lifecycle is a platform that helps organizations meet their security, regulatory, and business access needs, through a collaborative set of business processes. By automating manual access control tasks, providing access management workflows to gather the appropriate business approvals, and gathering evidence of compliance to access control policy, organizations can confidently manage, control, and enforce access to applications and data, across their organization. This functionality is enabled by a set of collectors that gather user and access information from various repositories and store it in a central data repository. RSA Identity Governance and Lifecycle also provides a set of data connectors to provision external data repositories with updated information. The RSA Identity Governance and Lifecycle platform contains functionality that is not covered by *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*. As with all evaluations claiming conformance to a NIAP-approved protection profile, only the functionality specified in the profile is evaluated.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product

[1] FTA_TAB.1 is included in the list of optional SFRs per TD0055 (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=58.)

satisfies all of the security functional and assurance requirements stated in the 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.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	RSA Identity Governance and Lifecycle v7.0.1
Sponsor & Developer	RSA The Security Division of EMC^2 10700 Parkridge Blvd. Suite 600 Reston, VA 20191
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	February 2017
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013, and including the following optional SFRs: FTA_SSL_EXT.1, FIA_AFL.1, FTA_SSL.3, FTA_SSL.4, and FTA_TAB.1.
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the RSA Identity Governance and Lifecycle v7.0.1.
Evaluation Personnel	Greg Beaver Cody Cummins Gary Grainger Kevin Steiner
Validation Personnel	Daniel Faigin, Senior Validator Stelios Melachrinoudis, Lead Validator Marybeth Panock, Validator

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) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	RSA Identity Governance and Lifecycle v7.0.1 Security Target
ST Version	1.0
Publication Date	April 11, 2017
Vendor	RSA The Security Division of EMC[2]
ST Author	Leidos
TOE Reference	RSA Identity Governance and Lifecycle v7.0.1
TOE Software Version	RSA Identity Governance and Lifecycle v7.0.1
Keywords	Identity and Credential Management

2.1 Threats

The ST references the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013, including the following optional SFRs: FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, and FTA_TAB.1[2], The protection profile identifies the following threats, which the TOE and its operational environment are intended to counter:

- An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
- A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
- 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.
- 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.
- 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.

[2] FTA_TAB.1 is included in the list of optional SFRs per TD0055 (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=58.)

- A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
- A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.
- A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
- A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

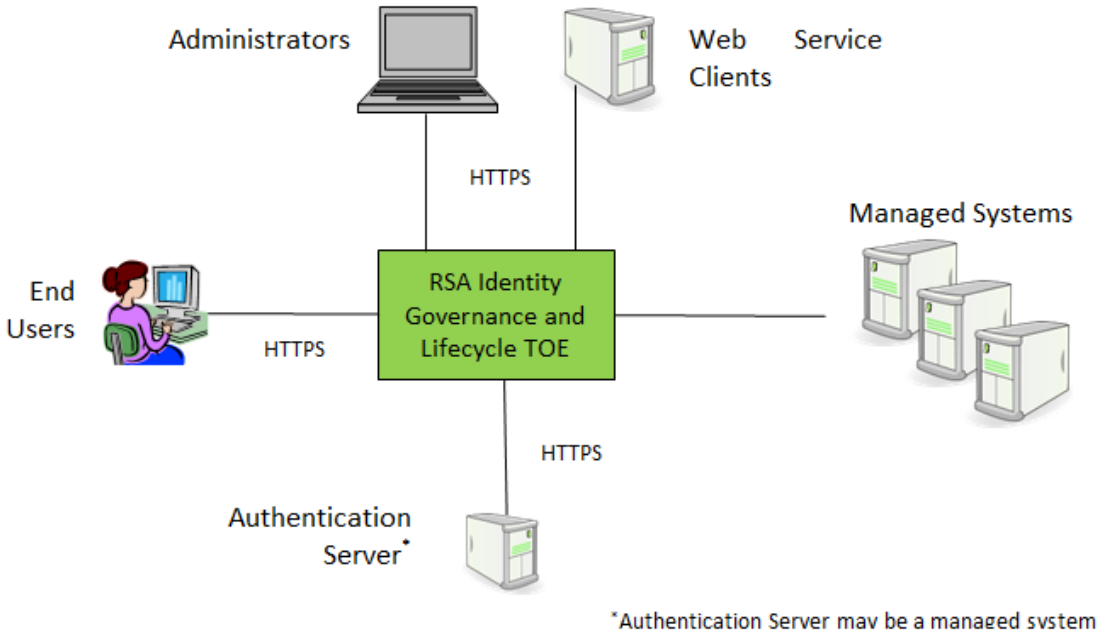
2.2 Organizational Security Policies

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

3 Architectural Information

The section describes the TOE architecture including physical and logical boundaries. Figure 1 shows the TOE in relation to its operational environment.

Figure 1 TOE Boundary



The TOE consists of the RSA Identity Governance and Lifecycle Software v7.0.1 and includes the following components:

- Access Certification Manager
- Business Role Manager
- Access Request Manager
- Rules
- Access Fulfillment Express (AFX)
- Collectors (agents)
- Graphical User Interface (GUI), and
- Web Services API.

The TOE includes connectors/collectors only for the Active Directory and Oracle data sources. Each of the Active Directory and Oracle data sources include the following data connector/collector types: Account, Identity, Entitlement, Role, and Application Metadata. AFX must be enabled in the evaluated configuration in order to automate the access request fulfillment process. Remote agents, the administrator workstations and web services clients are not part of the TOE.

4 Assumptions

The ST references the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013, to identify following assumptions about the use of the product:

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- There will be a defined enrollment process that confirms user identity before the assignment of credentials.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
- The TOE will receive reliable time data from the Operational Environment.

4.1 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs and scoped to those Security Functional Requirements (SFRs) declared in the ST. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. The TOE relies on the FIPS 140-2 validated BSAFE Crypto-J 6.2.1 in the operational environment for cryptographic functions. The TOE itself does not implement any cryptographic functions and, as such, the FCS requirements in the Architectural Variations section of the ESM ICM PP were not included in the ST, and were, therefore, not evaluated.
5. This evaluation did not specifically search for, nor attempt to exploit, 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.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Enterprise Security Management

The TOE maintains security attributes belonging to individual objects and relies on Active Directory in the operational environment to authenticate users.

The TOE provides the capability to define and securely transmit identity and credential data for use with other ESM products: Oracle and Active Directory authentication servers. The TOE provides a password restriction policy mechanism to ensure secure passwords are defined for enterprise users.

5.2 Security Audit

The TOE generates logs for security relevant events including the events specified in *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*. The TOE sends the logs to an Oracle database external to the TOE for storage. Reliable timestamps are provided by the operational environment.

5.3 Identification and Authentication

The TOE associates roles, entitlements, and other user attributes with enterprise users and relies on the operational environment to authenticate enterprise users.

5.4 Security Management

The TOE provides the management functions identified in the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management* such as management of subject attributes; authentication data; configuration and management of the security functions; and management of the users that belong to a particular role. The TOE restricts access to the management functions to users with the following roles: the System Administrator Role, Application Administrator Role, Password Management Role, Role Administrator Role, and Access Request Administrator Role and to users with entitlements to the functions. The TOE maintains all Administrator roles.

5.5 Protection of the TSF

Credentials/keys used by the TOE are stored in the operational environment. The TOE does not offer any interfaces to view the credentials/keys.

5.6 TOE Access

The TOE terminates local and remote interactive sessions after a System Administrator configurable time period of inactivity. It provides users the capability to terminate their own interactive sessions. An administrator can configure an advisory warning message regarding unauthorized use of the TOE, which the TOE displays before establishing a user session for the GUI.

5.7 Trusted Path/Channels

The TOE provides trusted communication channels using TLS v1.1 and TLS v1.2 for Active Directory authentication and transfer of policy data.

The TOE provides trusted communication paths using TLS v1.1 and TLS v1.2 for remote administrators and users accessing the GUI and for Web Service Clients accessing the Web Services API.

The TOE relies on BSAFE Crypto-J 6.2.1 in the operational environment for cryptographic functions. In particular, the module is used for TLS v1.1 and v1.2 connections with trusted external IT entities, and with users accessing the TOE.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. RSA provides electronic guidance documents by including the information in the consolidated Help files. Guidance documentation is accessible to customers inside and outside of the RSA Identity Governance and Lifecycle system. In particular, the following Common Criteria specific information is available:

- RSA Identity Governance and Lifecycle Supplemental Administrative Guidance V7.0.1
- RSA Identity Governance and Lifecycle7.0.1 Release Notes
- RSA Identity Governance and Lifecycle7.0.1 Installation Guide
- RSA Identity Governance and Lifecycle7.0.1 Upgrade and Migration Guide
- RSA Identity Governance and Lifecycle7.0.1 Help (Built-in Documentation)
- RSA Identity Governance and Lifecycle7.0.1 Database Setup and Management Guide
- RSA Identity Governance and Lifecycle7.0.1 Public Database Schema Reference
- RSA Identity Governance and Lifecycle Active Directory Application Guide, Version 1.1 | Nov 2016
- RSA Identity Governance and Lifecycle Connector Data Sheet for Oracle Database
- RSA Identity Governance and Lifecycle Collector Data Sheet for Oracle Database

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- *RSA Identity Governance and Lifecycle v7.0.1 Common Criteria Test Report and Procedures*, version 1.1, 14 April 2017

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013.

To this end, the evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the above-referenced Protection Profile.

The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the Leidos facility in Columbia, Maryland from September 26, 2016 to January 31, 2017.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory. As can be seen below, the configuration used during testing of the TOE matches that which was defined in the Security Target.

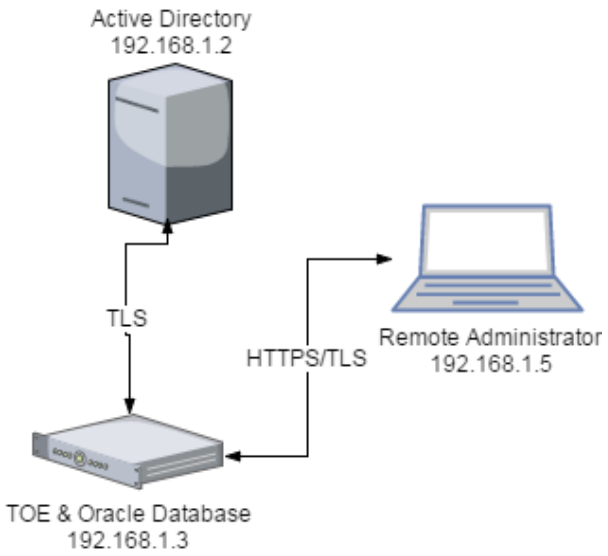


Figure 2 Test Configuration

As documented in the diagrams above, the following hardware and software components were included in the evaluated configuration during testing:

- The TOE application installed on a platform containing the following components:
  - Oracle DB v12.1.0.2
  - WebSphere Application Server (WAS) v8.5.5.2
  - IBM JDK 1.7

  - OpenJDK 7
  - BSAFE Crypto-J v6.2.1
  - SUSE Linux Enterprise OS 11 SP 3
  - General purpose hardware (x64 Intel Architecture)

- Non-TOE Components
  - Additional Oracle DB v12.1.0.2 for Directory Services running on the same platform as the TOE
  - Active Directory Running on Server 2012
  - Additional computer for Remote Administration through the Web GUI

The configuration used during testing of the TOE matches that which was defined in the Security Target. The evaluated version of the TOE was installed and configured according to the *RSA Identity Governance and Lifecycle7.0 Installation Guide* as well as the supporting guidance documentation identified in Section 6.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management,* Version 2.1, 24 October 2013 are fulfilled.

7.1 Penetration Testing

The evaluation team conducted an open-source search for vulnerabilities in the product. The open-source search did not identify any vulnerability applicable to the TOE in its evaluated configuration. No additional testing was required to verify the vulnerabilities were mitigated.

8 Evaluated Configuration

The evaluated version of the TOE is RSA Identity Governance and Lifecycle 7.0.1. The TOE must be deployed as described in section 4 Assumptions of this document and must be configured in accordance with *RSA Identity Governance and Lifecycle Supplemental Administrative Guidance V7.0.1* identified in section 6.

Per NIAP Policy Letter #22 (https://www.niap-ccevs.org/Documents_and_Guidance/policy.cfm), user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date. The product is still considered by NIAP to be in its evaluated configuration with such updates properly installed.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

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 in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ASE_CCL.1	Conformance Claims
ASE_ECD.1	Extended Components Definition
ASE_INT.1	ST Introduction
ASE_OBJ.1	Security Objectives
ASE_REQ.1	Security Requirements
ASE_TSS.1	TOE Summary Specification
ADV_FSP.1	Basic Functional Specification
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM Coverage
ATE_IND.1	Independent Testing - Conformance
AVA_VAN.1	Vulnerability Survey

10 Validator Comments/Recommendations

The security functionality that was evaluated was scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. The environment under which TOE is evaluated is scoped exclusively to that described in the "Evaluated Configuration of the TOE" section of *RSA Identity Governance and Lifecycle Supplemental Administrative Guidance V7.0.1*. All other functionality provided by the product, to include software or components that were not part of the evaluated configuration, need to be assessed separately and no further conclusions can be drawn about their effectiveness. Of note, additional functionality is covered in the online documentation *RSA Identity Governance and Lifecycle7.0.1 Help (Built-in Documentation)*[3].

This product, RSA Identity Governance and Lifecycle, is conformant to the Protection Profile for Enterprise Security Management (ESM) Identity and Credential Management, not the ESM Protection Profile for Access Control. This is relevant as there is a Rules Module that is a mechanism for maintaining a user module consistent with the organization's policies rather than access controls on managed systems. The Supplemental Administrative Guide contains a Rules Remediation section to explain this function.

The ST identifies security-relevant identity and credential attributes for enterprise users. The Admin Guide explains how to configure these attributes based on what is available for their business in RSA Identity Governance and Lifecycle and refers the user to the section of the Online Help 'Creating and Managing Attributes for RSA Identity Governance and Lifecycle Object'. This is noteworthy because a few of the attributes declared in the ST that enterprise users can be represented by can take on different names with equivalent meaning in practice. For example, while there is no explicit Credential Lifetime field for a user object, it is instead represented as Expiration Date. Another example is that Credential Status is represented by Is Terminated and Is Deleted fields, and Last Seen On is represented by the Last Login attribute.

The TOE relies on FIPS 140-2 validated BSAFE Crypto-J 6.2.1 (CMVP certificate #2468) in the operational environment for cryptographic functions. The cryptographic functions are used for all TLS connections with trusted external IT entities, and with users accessing the TOE. The TOE itself does not implement any cryptographic functions. Consequently, the Cryptographic Support (class FCS) requirements from the Architectural Variations section of the ESM ICM PP do not apply to the TOE. The ST does not claim any requirements from the FCS class and so the FCS requirements were outside the scope of evaluation and were not evaluated.

[3] The Validators received only a partial snapshot of the on-line guidance on 05-05-2017.

11 Annexes

Not applicable

12 Security Target

Name	Description
ST Title	RSA Identity Governance and Lifecycle v7.0.1 Security Target
ST Version	Version 1.0
Publication Date	April 11, 2017

13 Abbreviations and Acronyms

Abbreviation	Description
AAR	Assurance Activity Report
AFX	Access Fulfillment Express
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
ESM	Enterprise Security Management
ICM	Identity and Credential Management
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PCL	Product Compliant List
PP	Protection Profile
SAR	Security assurance requirement
SFR	Security functional requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
VR	Validation Report

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] *RSA Identity Governance and Lifecycle v7.0.1 Security Target*, Version 1.0, 11 April, 2017

[6] *RSA Identity Governance and Lifecycle v7.0.1 Common Criteria Test Report and Procedures*, version 1.1, 14 April 2017

[7] *RSA Identity Governance and Lifecycle v7.0.1 Common Criteria Assurance Activity Report*, Version 1.1, 5 May 2017

[8] *RSA Identity Governance and Lifecycle Supplemental Administrative Guidance v7.0.1 (undated)*

[9] Evaluation Technical Report For RSA Identity Governance and Lifecycle v7.0.1 (RSA Proprietary) Version 1.0 February 13, 2017

[10] Partial Snapshot of *RSA Identity Governance and Lifecycle7.0.1 Help (Built-in Documentation)5 May 2017.*