RSA Identity Governance and Lifecycle v7.0.1

Security Target

Version 1.0

April 11, 2017

Prepared for:

RSA The Security Division of EMC²

10700 Parkridge Blvd.

Suite 600

Reston, VA 20191

Prepared by:

leidos

Common Criteria Testing Laboratory

6841 Benjamin Franklin Drive, Columbia, Maryland 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is RSA Identity Governance and Lifecycle v7.0.1 provided by RSA. The RSA Identity Governance and Lifecycle product is an identity and access management solution intended to help organizations improve their information security and compliance by managing the user access lifecycle, including: initial access request; approval; fulfillment; review; certification; and remediation.

The Security Target contains the following additional sections:

- Product and TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – RSA Identity Governance and Lifecycle v7.0.1 Security Target

ST Version – Version 1.0

ST Date –4/11/2017

TOE Identification – RSA Identity Governance and Lifecycle v7.0.1

TOE Developer – RSA The Security Division of EMC[2]

Evaluation Sponsor – RSA The Security Division of EMC[2]

CC Identification – *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012*

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- *Standard Protection Profile for Enterprise Security Management Identity and Credential Management,* Version 2.1, 24 October 2013, [ESMICM] and including the following optional SFRs: FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, and FTA_TAB.1[1].
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012
    - Part 3 Conformant

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

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example, FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
- The [ESMICM] uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Abbreviations and Acronyms

ACL	Access Control List
AD	Active Directory
CC	Common Criteria for Information Technology Security Evaluation
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CR	Change Requests
DLP	Data Loss Prevention
FIPS	Federal Information Processing Standard
IT	Information Technology
ESB	Enterprise Service Bus
ESMICM	Standard Protection Profile for Enterprise Security Management Identity and Credential Management
J2EE	Java 2 Platform, Enterprise Edition
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format (LDIF)
PP	Protection Profile
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SA	Security Association

SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

2. Product and TOE Description

This section includes an overview of the RSA Identity Governance and Lifecycle solution, and then proceeds to identify the components which are included in the Target of Evaluation (TOE). The TOE description covers TOE architecture, logical boundaries, and physical boundaries.

2.1 Product Overview

RSA Identity Governance and Lifecycle is an identity and access management solution intended to help organizations improve their information security and compliance by managing the user access lifecycle, including: initial access request, approval, fulfillment, review, certification, and remediation. The solution provides a comprehensive, business-driven solution for identity management and governance across the Enterprise.

The RSA Identity Governance and Lifecycle solution provisions and manages access permissions that a user has to data and application resources in enterprise managed systems. The solution provides connector components to fulfill change requests on an endpoint (the managed system) and collector components that are used to gather information from data sources for management in RSA Identity Governance and Lifecycle.

The RSA Identity Governance and Lifecycle solution contains functionality that is not covered by the [ESMICM]. As with all evaluations claiming conformance to a Protection Profile, only the functionality specified in the PP is evaluated. This section describes the solution as a whole and Section 2.2 identifies the specific components and functionality included in the TOE.

The RSA Identity Governance and Lifecycle solution consists of the following components:

- Access Certification Manager;
- Business Role Manager;
- Access Request Manager;
- Data Access Governance;
- Rules;
- Access Fulfillment Express (AFX);
- Collectors (agents);
- GUI; and
- Web Services API.

RSA Identity Governance and Lifecycle provides the capability to automatically collect identity, account, group, role, and entitlement information across both application and data resources. An Account is defined as a logon account that provides access to one or more applications. Users can have multiple accounts, and accounts can be shared by multiple users. The solution supports data collection from many data sources such as Active Directory, databases, files, ACLs, J2EE, LDAP, LDIF, and WebLogic.

RSA Identity Governance and Lifecycle is capable of enrolling enterprise users and assigns uniquely identifying data that is associated with the users and their defined security-relevant attributes. RSA Identity Governance and Lifecycle provides methods and combinations to accomplish this including the use of data collection agents in combination with Account Templates, Account Creation Forms, and Account Password Policies.

Custom user attributes can be created and mapped to source data attributes for users in the organization and managed locally in RSA Identity Governance and Lifecycle. For example, the user may want to add a collectible security code attribute or a locally managed notes attribute or any number of other attributes that is considered significant to maintaining compliance with access governance objectives. Custom user attributes are outside the scope of the evaluation.

The RSA Identity Governance and Lifecycle agent is a client software component that provides a framework for data collectors to operate under and manages a constant network connection with the RSA Identity Governance and Lifecycle server. The default local agent “AveksaAgent” is built directly into the server. In some deployment scenarios, however, additional agents may be required to be installed and configured on remote machines due to network access restrictions that prevent the server-based agent from communicating directly with data sources. The solution creates and maintains certificates and keystores for secure communication of the agent and the TOE server platform.

The Business Role Manager module provides Enterprise role management allowing organizations to verify and enforce regulatory mandates and to audit the effectiveness of user access policies. Role management is a critical component in addressing governance and compliance requirements for user access to mission-critical applications and data. Roles support compliance by aligning access privileges to user job functions within the organization and by providing business context to lower-level entitlements and permissions, which need to be reviewed by business managers and compliance staff. Business Role Manager's role lifecycle management features permit the user to create and verify role-based access across enterprise applications. Aggregating user access privileges under roles improves entitlement management and ensures that access rights adhere to business and regulatory policies. Ensuring adherence to these policies requires that business managers and auditors review and certify that user access privileges are appropriate within the organization. Business Role Manager enables users to identify policy violations and inappropriate access and take corrective actions when necessary.

The Access Certification Manager module enables business managers and other personnel with oversight responsibility over who has access to resources in the organization to determine whether users have appropriate access to the resources they require to do their jobs. This capability is provided through the User Access Certification Reviews process. The TOE provides enterprise-level visibility into what entitlements, permissions, and accounts users have and what groups and roles they belong to and enable business managers to review and maintain or revoke the entitlements and memberships and certify the results. The TOE's central repository keeps a historical trend of all the data it collects to let users see what access employees have at a particular point in time or how the collected information (for example, user entitlements) has changed over time.

The Access Request Manager module enables line-of-business managers, supervisors, asset owners, and other users to request access and request changes to entitlements to resources in an organization for themselves and other users. It also provides request management capabilities that enable users to customize how access is requested, create views of request activities (approvals and fulfillments) for business users who require monitoring capabilities over those activities, and specify policies for account password reset requests and manage challenge questions for login password reset requests.

The Rules module must be implemented on the system to provide decision support rules for access requests. All content related to business rules and violating access pertaining to the Access Request Manager is applicable only if the Rules module is implemented on the system. The TOE allows creation of process business rules that detect and provide notifications for various conditions reflected in collected data that users want to monitor and possibly rectify to maintain compliance with the organization's security and regulatory policies. For example, a user can configure a rule to detect whether users in a particular location or that belong to a particular business unit or department are able or are not able but should be able to access a particular application resource.

Rules can also serve to provide decision support in user access request and role modeling processes. For example, RSA Identity Governance and Lifecycle would use a rule to evaluate an entitlement access request for a user to determine whether the request grant would violate a business rule if it were granted. Rules are written so that a match indicates a business policy violation. A rule violation occurs when a user entitlement matching a rule's condition is detected in the solution's data store. The solution enforces compliance policies for users, groups, and objects, and determines if rules would be violated. The user attribute Violation Count is the number of rule violations registered for the user and is maintained by the Rules module. RSA Identity Governance and Lifecycle enables particular users (a line of business manager or a IT security officer for example) to create and process business rules that detect and provide notification of various conditions reflected in collected data that are monitored. A multitude of rules can be written.

A subset of conditions that can be detected with rules include:

- Users have entitlements they should not have
- Users do not have entitlements they should have
- Users have entitlements that violate segregation of duties rules
- User attributes have changed, which indicate that users have joined, moved within, or left the organization
- User entitlement changes
- Role membership and role metrics changes

Entitlements in the context of a business rule include:

- Directly granted entitlements and entitlements granted through accounts

- Directly granted application roles
- Memberships in groups and roles and the entitlements, sub-roles, application roles, and accounts indirectly granted to users as a result of their memberships

The Data Access Governance module provides visibility, monitoring, certification, remediation, and reporting of user access permissions to data stored on Microsoft Windows file servers, network-attached storage devices and Microsoft SharePoint servers. This module:

- Provides visibility into Data Resources such as who owns enterprise data resources, who has access to what data resources, how they get access; and who approved it.
- Provides enforcement of Compliance Policies consisting of business rules that enable creation and enforcement of compliance policies for users and groups.
- Leverages existing Microsoft AD (Active Directory) groups. Data classifications from DLP (Data Loss Prevention) systems can determine controls and use for access risk management processes.

The Access Fulfillment Express (AFX) module automates the access request fulfillment process. Where RSA Identity Governance and Lifecycle supports the business logic associated with access request fulfillment requirements, AFX executes the fulfillments at the target endpoints. The AFX module uses connectors to fulfill change requests on an endpoint. The system uses collected data to verify that a connector fulfillment activity was completed. The AFX module provides a set of connector templates for a variety of data sources such as Active Directory, and Oracle database for which connectors can be created. Each connector type includes a set of fulfillment commands that can be completed on an endpoint. AFX is RSA's approach to fulfilling access changes that stem from access governance business processes (such as reviews, role management, access requests, and joiner, mover, and leaver processes). AFX must be enabled in order to automate the access request fulfillment process. If AFX is not enabled, users can manually implement the fulfillment of requests by directly connecting to the data sources and updating the information. The evaluation covers the automated provisioning case, which satisfies the requirements in the protection profile. Manual fulfillment has the same intention but, given it is manual, does not directly satisfy the requirements in the protection profile and is not considered for this evaluation.

RSA Identity Governance and Lifecycle maintains three types of administrators: the AveksaAdmin Administrator; users with an entitlement granting a particular privilege; and the Application Administrator roles. The Application Administrator roles consist of System Administrator; Password Management Role; Role Administrator; and Access Request Administrator. AveksaAdmin users or users with the System Administrator role are authorized to manage all aspects of the TOE including defining and managing identity, credential, and object attributes. The AveksaAdmin user account is used only during initial installation and configuration. Guidance documentation instructs RSA Identity Governance and Lifecycle customers to change the password for the AveksaAdmin account and to assign a user the System Administrator role instead. The solution also offers additional predefined roles as well as entitlements that provide a subset of management functionality. Administrators can grant administrative privileges called entitlements directly to other users, to groups and to roles. Users that are a member of a group, are assigned the role, or have an account will obtain the entitlement(s) assigned to that group, role or account.

The solution provides a graphical user interface (GUI) that includes management functions for both business users and security administrators of the RSA Identity Governance. It also provides a Web Services API that enables authorized users to issue HTTP GET and POST calls to invoke security management functions. The GUI provides all management functions of the TOE. Both require the authorized user to be identified and authenticated prior to access and to have the appropriate entitlement or role. The API calls can be issued via a Representational State Transfer (REST) client, custom code, or external programs.

Web Services client applications for the Android and iPhone mobile platforms (phones, not tablets) enable users to access and complete their change request approvals from their mobile devices. Supported versions are Android 2.1 or greater; and iPhone iOS 5.0 or greater. In the evaluated configuration, the Web Services API is accessed via Web Services Clients in the operational environment.

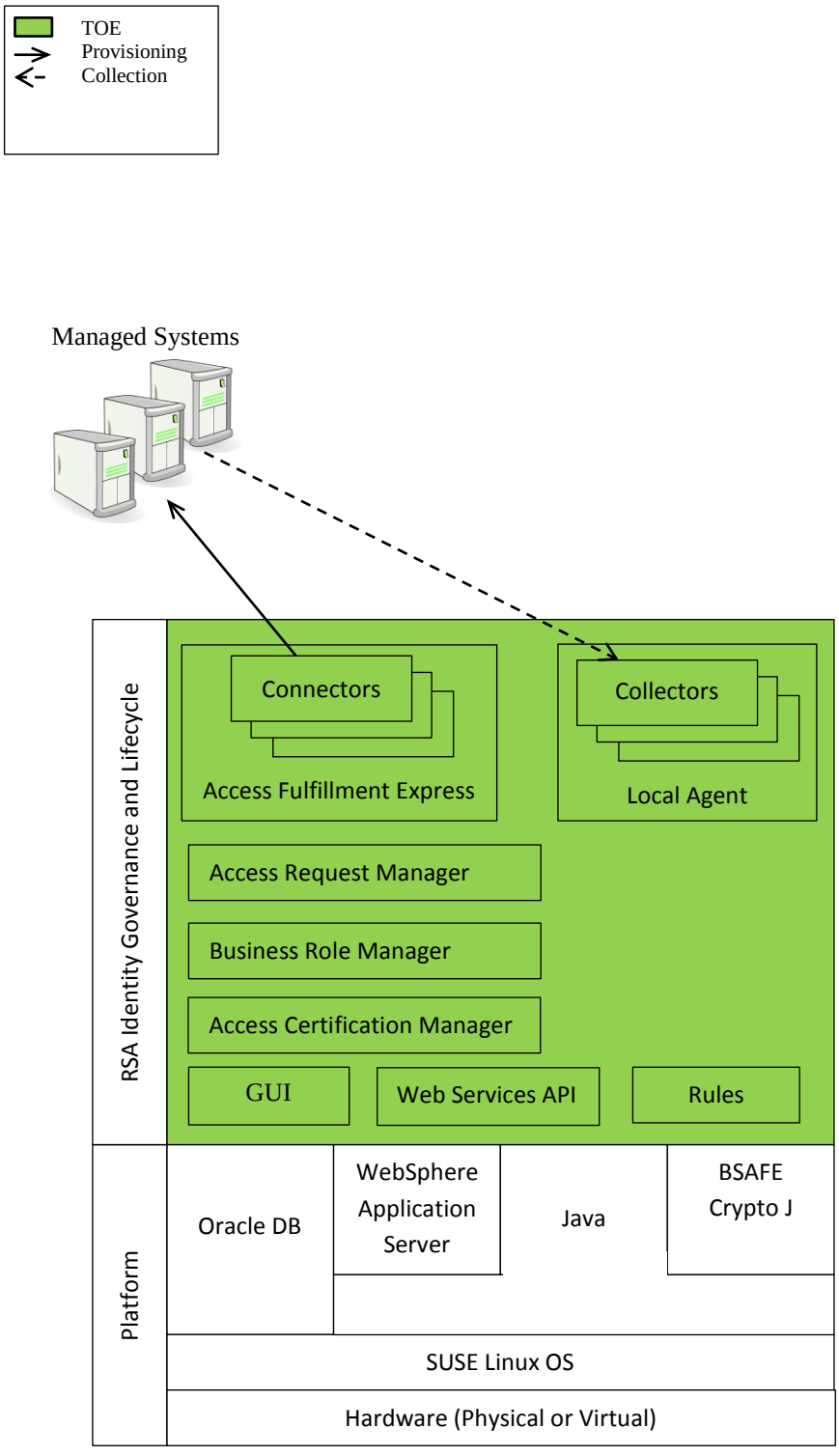
2.2 TOE Overview

The TOE consists of the following components:

- Access Certification Manager;
- Business Role Manager;
- Access Request Manager;
- Rules;
- Access Fulfillment Express (AFX);
- Collectors (local agents);
- GUI; and
- Web Services API.

Each component contributes to the security functions of the TOE with the exception of the Rules component. The Rules component is a mechanism for maintaining a user model consistent with the organizations policies (rather than implementing access controls on managed systems). As such, the rules module is included in the evaluated configuration but does not support any of the claimed security functionality identified in the PP and is therefore not evaluated.

Figure 1 RSA Identity Governance and Lifecycle Platform and TOE



The TOE components identified above collectively provide functionality defined in the [ESMICM]. Specifically the functionality included in the evaluation is:

- Provision 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)
- Enforce password strength rules for enterprise users
- Establish appropriate trusted channels between itself 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

RSA Identity Governance and Lifecycle provides the System Administrator role for granting other users administrator entitlements or roles. The TOE provides its users access by defining an Active Directory authentication source. The TOE collects user information from specified Active Directory authentication sources that contain log on credentials for the users. These authentication sources authenticate enterprise users using password authentication and communication with the authentication sources is protected using TLS. Users must be authenticated prior to accessing any security functionality through either the GUI or the Web Services API. The Web Services API enables authorized users to issue HTTP GET and POST calls to invoke security management functions. Additionally, the TOE offers a GUI that also provides security management functions to manage the TOE.

Communication between the users and the TOE is protected using TLS.

The TOE provides access protection functions such as configurable advisory warning message, and session inactivity termination. The TOE enforces password strength policies for enterprise user credentials that specify password composition strength rules including a settable password minimum length (minimum of 15 or greater is supported). The policies are configurable by an authorized administrator.

Audit events are generated and logged in the Oracle database (in the operational environment) and can be accessed from the Application Log Administration window in the GUI which allows Administrators to view the audit records. Some audit records can be accessed from CR (Change Requests) history and activity log and system logging. Change requests can be viewed in the system during (while active or in-progress) or after they are completed. The logs identify the user(s) who submitted and approved the request along with other details including when and how the request was fulfilled.

The TOE uses its Access Certification Manager and Collector components to collect identity, account, group, role, and entitlement information from enterprise sources. The TOE includes data collection from Active Directory and Oracle database sources only. The TOE then generates a unique identifier for each user and associates the user and the user's credentials with the unique identifier.

The RSA Identity Governance and Lifecycle TOE provisioning of users entails enrolling new subjects to an organizational repository, and associating and disassociating subjects with organizationally-defined attributes. The Access Fulfillment Express (AFX) and Connector components serve to automatically fulfill change requests on an endpoint (Active Directory and Oracle). RSA Identity Governance and Lifecycle creates and maintains certificates and keystores for secure communication using TLS between the managed systems and the TOE and between the Collectors (local agents) and the TOE's server platform.

The Business Role Manager component permits the user to create and verify role-based access across enterprise applications. Aggregating user access privileges under roles improves entitlement management.

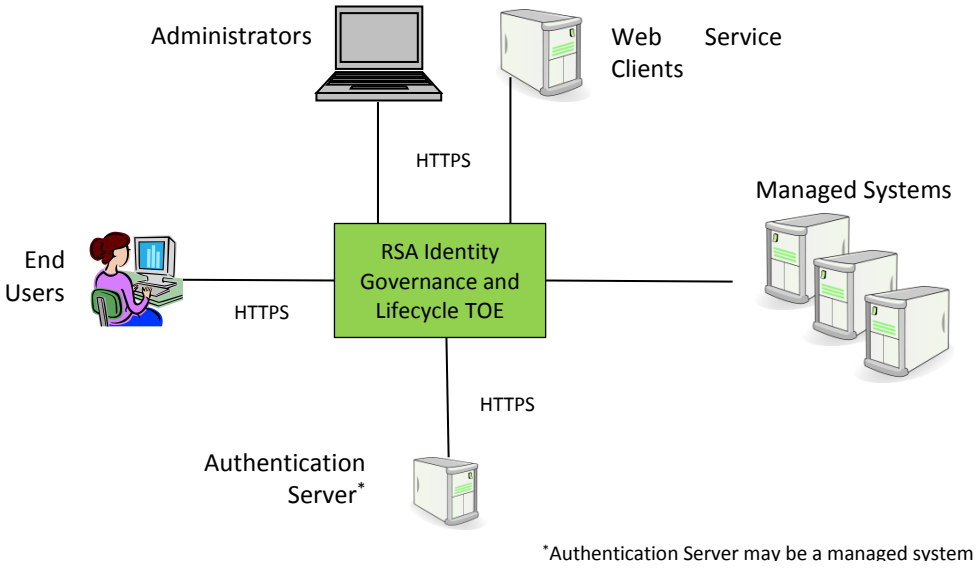
The Access Request Manager component allows users to request access and request changes to entitlements to resources in an organization for themselves and other users. This component also provides authorized administrators with the capability to approve the change requests, specify policies for account password reset requests and manage challenge questions for login password reset requests. Authorized administrators use the GUI and the Web Services API to manage the TOE including the entitlements granted to users. Authorized users can create and approve requests for user entitlement or to be added to an account or a role that has particular entitlements using the Access Request Manager and Business Role Manager components.

The TOE relies on FIPS 140-2 validated BSAFE Crypto-J 6.2.1 in the operational environment (CMVP certificate # 2468), for cryptographic functions. The cryptographic functions are used for all TLS connections with trusted external IT entities, and with users accessing the TOE.

2.3 TOE Architecture

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

Figure 2 TOE in Operational Environment



2.3.1 Physical Boundaries

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), GUI, and Web Service API. The evaluation boundaries are restricted to the Active Directory and the Oracle databases and therefore the Data Access Governance component is not included in the TOE. As described in the Product Overview section, the TOE provides the capability to automatically collect identity, account, group, role, and entitlement information across both application and across data resources. The TOE includes connectors/collectors only for the Active Directory and Oracle data sources. Each of the AD 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.

The TOE is deployed as a software application running on a WebSphere application server: referred to as the 'WebSphere' Installation in the installation guide. The TOE is RSA Identity Governance and Lifecycle v7.0.1 installed on a platform consisting of:

- Oracle DB v12.1.0.2
- WebSphere Application Server (WAS) v8.5.5.2
- Java JDK v1.7
- OpenJDK 7 (JRE 7.0)
- BSAFE Crypto-J v6.2.1

- SUSE Linux Enterprise OS 11 SP 3,
- Hardware: See Section 2.3.1.2

The OS, the database, WAS, Java, hardware and the BSAFE Crypto-J modules are considered to be the in the operational environment.

An RSA Identity Governance and Lifecycle agent is a client software component that provides a framework for data collectors to operate under. An agent manages a constant network connection with the server. The default local agent "AveksaAgent" is built directly into the server. Remote Agents are not included in the TOE. The TOE creates and maintains certificates and keystores for secure communication of the agent and the TOE server platform.

The TOE relies on FIPS 140-2 validated BSAFE Crypto-J 6.2.1 (CMVP certificate #2468) in the operational environment for cryptographic functions.

Reliable timestamps used by the TOE (in audit record timestamps for example) are provided by the operational environment.

2.3.1.1 Software Requirements

The TOE requires compatible software to be installed on client machines in order to access the GUI and the Web Services API. All major web browsers are supported, including IE 10+, Firefox v30+, Chrome v31+, and Safari v8.x.

2.3.1.2 Hardware Requirements

Hardware can be physical or virtual. For typical enterprise deployments up to 500 concurrent users, up to 1000 applications, and up to 20 million entitlements the following requirements apply.

- x64 Intel Architecture
- System memory: Minimum 16GB RAM, 32GB recommended
- Storage: At least 1TB of usable disk space ideally using serial-attached SCSI drives or other high performance drives

The TOE requires the following ports to be available for use:

- 8080: RSA Identity Governance and Lifecycle application server HTTP port
- 8443: HTTPS port for web browsers and web services
- 8444: HTTPS port for agents and the AFX server
- 8445: HTTP port for the RSA Identity Governance and Lifecycle application workflow compiler (internal use only)

WebSphere requires the following hardware:

- Memory: System meets the hardware requirements specified for the version of WebSphere Server used, with sufficient excess memory to meet the RSA Identity Governance and Lifecycle requirements. RSA recommends that the following minimum amounts of system memory available for the application: 4GB for development environments, 8GB for production environments, and up to 32GB for environments with up to 300 concurrent users.
- Temporary disk space: WebSphere deployment of RSA Identity Governance and Lifecycle requires 1GB of /tmp space, 2GB recommended.
- The application server disk requires sufficient space for the deployed RSA Identity Governance and Lifecycle application and runtime data. While the application only requires 300MB, data collections can require several GB of space. 5GB is the recommended minimum. Actual size requirements for collections are dependent on usage.

The TOE requires an AD authentication server(s) in the operational environment for authentication of users and administrators.

2.3.2 Logical Boundaries

This section summarizes the security functions provided by RSA Identity Governance and Lifecycle:

- Enterprise security management
- Security audit
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

2.3.2.1 Enterprise Security Management

The TOE maintains security attributes belonging to individual objects and relies on AD 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 AD authentication servers. The TOE provides a password restriction policy mechanism to ensure secure passwords are defined for enterprise users.

2.3.2.2 Security Audit

The TOE generates logs for security relevant events including the events specified in ESMICM PP. The TOE sends the logs to an Oracle database external to the TOE for storage. Reliable timestamps are provided by the operational environment.

2.3.2.3 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.

2.3.2.4 Security Management

The TOE provides the management functions identified in the ESMICM PP 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. See FMT_MOF.1 for a complete list management functions. The TOE restricts access to the management functions to users with the following roles: the System 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.

2.3.2.5 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.

2.3.2.6 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 using the GUI.

2.3.2.7 Trusted Path/Channels

The TOE provides trusted communication channels using TLS v1.1 and TLS v1.2 for AD 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.

2.4 TOE 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 Lifecycle 7.0.1 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*

3. Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) with the optional assumptions: A.CRYPTO, A.ROBUST, and A.SYSTIME from the [ESMICM].

In general, the [ESMICM] has presented a Security Problem Definition appropriate for enterprise security identity and credential management products, and as such are applicable to the RSA Identity Governance and Lifecycle TOE.

4. Security Objectives

Like the Security Problem Definition, this security target includes by reference the Security Objectives from the [ESMICM]. The [ESMICM] security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the [ESMICM] has presented a Security Objectives statement appropriate for enterprise security identity and credential management products, and as such are applicable to the RSA Identity Governance and Lifecycle TOE.

4.1 Security Objectives for the Environment

OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject 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. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile (PP): *Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013,* [ESMICM]. As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the [ESMICM] made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in [ESMICM].

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [ESMICM]. The [ESMICM] defines the following extended SFRs and since they are not redefined in this ST, the [ESMICM] should be consulted for more information in regard to those CC extensions.

- 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_STG_EXT.1: External Audit Trail Storage
- FPT_APW_EXT.1: Protection of Stored Credentials
- FPT_SKP_EXT.1: Protection of Secret Parameters
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE.

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_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 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
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path

Table 1 TOE Security Functional Components

5.2.1 Enterprise Security Management (ESM)

5.2.1.1 Reliance on Enterprise Authentication (ESM_EAU.2)

ESM_EAU.2.1 The TSF shall rely on [***ADJ***] for subject authentication.

ESM_EAU.2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

5.2.1.2 Reliance on Enterprise Identification (ESM_EID.2)

ESM_EID.2.1 The TSF shall rely on [***ADJ***] for subject identification.

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

5.2.1.3 Identity and Credential Definition (ESM_ICD.1)

ESM_ICD.1.1 The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2 The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, **[name (first and last), User ID, Title, Job Status, Supervisors, Department and Business Unit, First Seen On, Last Seen On, Is Deleted, Is Terminated, Termination Date, Unique Id, Account, Group, Role and Entitlement]**.

ESM_ICD.1.3 The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4 The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5 The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8 The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

a) For password-based credentials, the following rules apply:
   1. Passwords shall be able to be composed of a subset of the following character sets: **[English character set]** that include the following values **[26 uppercase letters, 26 lowercase letters, 10 numbers, and the following 10 special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"**]; and
   2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and
   3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and
   4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:
   1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

5.2.1.4 Identity and Credential Transmission (ESM_ICT.1)

ESM_ICT.1.1 The TSF shall transmit [***identity and credential attribute data***] to compatible and authorized Enterprise Security Management products under the following circumstances: [***immediately following creation or modification of data***].

5.2.2 Security Audit (FAU)

5.2.2.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

1) Start-up and shutdown of the audit functions; and
2) All auditable events identified in Table 2 for the not specified level of audit; and
3) [**no other auditable events**].

Requirement	Auditable Events	Additional Audit Record Contents
ESM_EAU.2	All use of the authentication mechanism	None
ESM_ICD.1	Creation or modification of identity and credential data	The attribute(s) modified
ESM_ICD.1	Enrollment or modification of subject	The subject created or modified, the attribute(s) modified (if applicable)
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed
FTA_SSL.3	All session termination events	None
FTA_SSL.4	All session termination events	None
FTA_SSL_EXT.1	All session locking and unlocking events	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

Table 2 Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

1) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**information specified in column three of Table 2**].

5.2.2.2 External Audit Trail Storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [**Oracle database**].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

1) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and
2) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 User-Subject Binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**all user security attributes**].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**successful user authentication provides for the initial association of attributes].**

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**user attributes cannot be changed within a session; within a session, if a request to change administrator attributes requires additional approval and the request has been approved by an authorized administrator; then the TSF changes an administrator's attributes**].

5.2.4 Security Management (FMT)

5.2.4.1 Management of Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***determine the behavior of, disable, enable, modify the behavior of***] the functions: [**list of functions in Table 3**] to [**Entitlement/Role identified in Table 3**

Requirement	Management Activities	Entitlement/Role	Operation
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	System Administrator Role **Entitlements:** Reset Password:Admin User:Manage User Attribute:Edit Web Services:Admin	Determine/modify the behaviour of
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	System Administrator Role **Entitlements:** Reset Password:Admin User:Manage User Attribute:Edit Web Services:Admin	Determine/modify the behaviour of
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	System Administrator Role Role Administrator Role	Determine/modify the behaviour of: Full control over establishment, removal etc.. of enterprise user's (maintained in the TOE) and their credentials including the ability to activate (or define a user) and assign users to roles.
		Access Request Administrator Role– can perform all of the capabilities	Enable, Disable, Determine/modify the behaviour of: Full control over user's credentials including ability to activate, assign and revoke roles, accounts, and entitlements
		Password Management Role-password management feature	Enable, Disable,Modify the behaviour of the password management function

Requirement	Management Activities	Entitlement/Role	Operation
		Entitlements provide a subset of capabilities as follows: • Account:Edit • Account Collector:Edit • Group:Edit • Role:Edit Members • Change request: Edit • Change Approval:Edit •	Determine/modify the behaviour of: Edit constitutes: Add and remove operations. For example; Account: Edit includes Add users to and remove users from accounts.
		• Account Collector:Manage • Role:Manage • Change Request:Edit • Change Approval: :Edit	Determine/modify the behaviour of: Manage constitutes the edit functions along with create and manage the attribute values. For example Role:Manage allows for add, and removing users from roles; and for managing the role.
		• Account Collector:Admin • Role:Admin • Change request:Edit • Change Approval:Edit	Determine/modify the behaviour of/ Enable,Disable,Modify:: The Admin entitlement provides a user with full capabilities.
ESM_ICD.1	Management of credential status	System Administrator Role Access Request Administrator Role	Modify the behavior of
ESM_ICD.1	Enrollment of users into repository	System Administrator Role Access Request Administrator Role	Determine the behavior of
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data is performed	System Administrator Role **Entitlement:** Authentication:Admin (manage authentication sources)	Determine/modify the behaviour of Enable/Disable
FAU_STG_EXT.1	Configuration of external audit storage location	performed during installation and set-up	Enable, disable.
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	See ESM_ICD.1	

Requirement	Management Activities	Entitlement/Role	Operation
FMT_MOF.1	Management of sets of users that can interact with security functions	System Administrator Role	Determine/modify the behavior of
FMT_SMR.1	Management of the users that belong to a particular role	System Administrator Role Role Administrator Role Access Request Administrator Role– can perform all of the capabilities Entitlements provide a subset of capabilities as follows: • Role:Edit Members • Role:Manage • Role:Admin • Change Request:Edit • Change Approval:Edit	see "ESM_ICD.1 - Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)" above which includes a description of the correspondence between roles/entitlements and operations for this function.
FTA_SSL.3	Configuration of the inactivity period for session termination	System Administrator Role **Entitlement:** Admin Security:Admin entitlement System:Admin entitlement	Determine/modify the behaviour of Enable/Disable
FTA_SSL_EXT.1	Configuration of the inactivity period for session termination	System Administrator Role Entitlement: Admin Security:Admin entitlement System:Admin entitlement	Determine/modify the behaviour of Enable/Disable
FTA_TAB.1	Maintenance of the banner	System Administrator Role **Entitlements:** Authentication:Admin entitlement System:Edit entitlement	Enable/Disable the banner including defining the message that will be displayed.
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	System Administrator Role	Enable/Disable
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	System Administrator Role	Enable/Disable

Requirement	Management Activities	Entitlement/Role	Operation

Table 3 TOE Management Functions

5.2.4.2 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**the management functions identified in Table 3**].

5.2.4.3 Security Management Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**System Administrator, Password Management Role, Role Administrator, and Access Request Administrator**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 Protection of Stored Credentials (FPT_APW_EXT.1)

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

5.2.5.2 Protection of Secret Key Parameters (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.2.6 TOE Access (FTA)

5.2.6.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after an [Authorized Administrator-configurable time interval of session inactivity].

5.2.6.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.2.6.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [***terminate the session***] after an Authorized Administrator specified time period of inactivity.

5.2.6.4 TOE Access Banner (FTA_TAB.1)

FTA_TAB.1.1 Before establishing a user session, the TSF shall display a configurable advisory warning message regarding unauthorized use of the TOE.

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 Trusted Channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall use [***[TLS 1.1[2] (RFC 4346), TLS 1.2 (RFC 5246) from the operational environment]***] to provide a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2 The TSF shall permit [***the TSF]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for transfer of policy data, [**AD authentication**].

5.2.7.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall use [***[TLS 1.1[2] (RFC 4346), TLS 1.2 (RFC 5246) from the operational environment]***] to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification, disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, execution of management functions.

[2] BSAFE Crypto-J 6.2.1 CMVP certificate #2468 includes by reference CAVP CVL certificate #471 for TLS.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the [ESMICM].

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 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 4 Assurance Components

Consequently, the assurance activities specified in [ESMICM] apply to the TOE evaluation.

6. TOE Summary Specification

This chapter describes the security functions:

- Enterprise security management
- Security audit
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Enterprise Security Management

The TOE maintains user security attributes and relies on AD in the operational environment to authenticate the users.

The TOE provides the capability to define and securely transmit identity and credential data for use with other ESM products in particular AD authentication servers. The TOE provides a password restriction policy mechanism to ensure secure passwords are defined.

6.1.1 ESM_EAU.2/ ESM_EID.2

The TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject. The TOE users are authenticated using Active Directory in the operational environment. AD authentication sources that contain user or subject logon credentials are specified and those sources are associated with the account collectors or identity collectors that collect the data from the sources.

6.1.2 ESM_ICD.1

The TOE provides the capability to define identity and credential data for use with AD servers and Oracle databases, via Account Templates and Account Creation Forms. The TOE is capable of defining the following default security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status (that is, Active Status (Active or terminated)), name (first and last), User ID, Title, Job Status, Supervisors, Department and Business Unit, First Seen On, Last Seen On, Is Deleted, Is Terminated, Termination Date, Unique Id, Account, Group, Role and Entitlement. The credential lifetime attribute is represented on the TOE as Expiration Date. The credential status is represented as two fields, Is Terminated and Is Deleted, both of which can be given values of yes or no. The Last Seen On attribute is viewed on the TOE as Last Login.

The TOE collects a user ID from an external source that represents the user. The TOE also has an internal ID for each user. This internal ID (unique ID) helps define how the representation of a user in one external system maps to the

same user in a different external system. For example, there might be a user: fsmith on one system and a user: fred.smith@acme.com on another system. The unique ID and defined resolution rules serves to link the two. The TOE associates the user and the user's credentials (including User ID) with the unique identifier.

Security attribute data is collected from the managed systems for use in defining policies and then provisioned to managed systems for enforcement.

The TOE uses its data collection agents for enrolling enterprise users and assigns uniquely identifying data that is associated with the users and their defined security-relevant attributes.

The TOE allows authorized administrators and users on remote AD Authentication Servers and managed systems to update an enterprise user's credentials. The TOE has the ability to detect external changes to passwords and can request a password reset on external user accounts. The TOE's provisioning and automatic fulfilment capability of AFX processes approved change requests (to change password for example), that are then fulfilled by the AD and Oracle database ESM.

The TOE provides the capability to revoke an enterprise user's credentials, either by requesting a password reset or an account action, such as disabling or locking an account, or terminating the user.

The TOE provides the capability to ensure defined enterprise user credentials satisfy specified minimum strength rules, via Password Policies. Password Policies can be defined for all users and enforces the following:

- Password strength — Minimum password length and alphanumeric character requirements and restrictions (as specified in ESM_ICD.1.8).
- Password history — The number of passwords that have been previously reset that cannot be used in a password reset.
- Password expiration — The number of days before an account password automatically expires.

The TOE supports administrative configurable minimum password lengths including those consisting of 15 characters or greater.

6.1.3 ESM_ICT.1

The TOE transmits identity and credential attribute data to compatible and authorized AD ESM and Oracle database products as part of Access Request processing, using the automatic fulfilment capability of AFX. AFX automatically propagates the data to the managed system.

Credentials are transmitted during login and during Change Request fulfillment (reset password fulfillment in particular) in order to synchronize credentials on the external AD or Oracle database. In addition, other attributes are passed to the endpoint to perhaps change group membership as an example. The fulfillment process can change any of the user attributes except for granular entitlements associated with a resource. These are maintained by the application owner in the ESM system.

6.2 Security Audit

The TOE generates logs for security relevant events including the events specified in ESMICM PP. The TOE sends the logs to an Oracle database external to the TOE for storage. Reliable timestamps are provided by the operational environment.

6.2.1 FAU_GEN.1

The TOE generates log records for security relevant events as they occur. The events that can cause an audit record to be logged include the following auditable events defined in **Table 2**:

- Startup and shutdown of the audit functions
- All use of the authentication mechanism
- Creation or modification of identity and credential data
- Enrollment or modification of subject
- All attempts to transmit information
- Establishment and disestablishment of communications with audit server

- All modifications of TSF function behavior
- Use of the management functions
- All TSF-initiated session termination events
- All Administrator-initiated session termination events
- All use of trusted channel functions
- All attempted uses of the trusted path functions

The logged audit records identify the date and time, the nature or type of the triggering event, an indication of the outcome of the event, and the identity of the user responsible for the event. The logged audit records also include event-specific content that includes at least all of the content required in **Table 2**.

6.2.2 FAU_STG_EXT.1

The TOE stores audit records in the operational environment on the Oracle database installed with the TOE. The database is installed on the same machine as the TOE and therefore a secure communication connection is provided by direct, platform-internal channel rather than cryptographic protocols. This architecture prevents the possibility of audit loss due to broken networked channel connections; and ensures all audit records generated are indeed stored in the audit log.

The storage of generated audit data is in the operational environment and therefore the TOE relies on the environment to protect the stored audit records from unauthorized deletion; and to prevent unauthorized modifications to the stored audit records in the audit trail.

6.3 Identification and Authentication

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

6.3.1 FIA_USB.1

The TOE associates all of the users security attributes with subjects acting on the behalf of that user. Users receive their privileges through assignment of entitlements either directly; through account definition or by way of membership in groups and/or roles. Attribute changes for users are not immediate and require a log-off and log-in. All enterprise users (including those that have administrative privileges) are also associated with the following user attributes during Identity Collection/Provisioning: credential lifetime, credential status (that is, Active Status (Active or terminated)), name (first and last), User ID, Title, Job Status, Supervisors, Department and Business Unit, First Seen On, Last Seen On, Is Deleted, Is Terminated, Termination Date, Unique Id.

The TOE enforces the following rule on the initial association of user security attributes with subjects acting on the behalf of users: users must be successfully authenticated for the initial association of attributes to occur.

The TOE enforces the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

- user attributes cannot be changed within a session, and
- administrator attribute changes in a session can be requested using the access request function.

To request a new access change the user can request entitlement access and removal of entitlement access through the Manage Access on the user's home page dashboard. An Access Request is created and if the request requires additional approval then the request must be approved by an authorized administrator.

6.4 Security Management

The TOE provides the management functions identified in the ESMICM PP; maintains roles and restricts access to the functions. The management functions are restricted to users with the entitlement granting the privilege, and to users with Application roles that provide administrative capabilities. The Application roles that provide administrative

capabilities include System Administrator, Password Management Role, Role Administrator and Access Request Administrator.

6.4.1 FMT_MOF.1

The TOE restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the management functions as defined in Table 3.

6.4.2 FMT_SMF.1

The TOE provides the management functions identified in **Table 3**

6.4.3 FMT_SMR.1

The TOE maintains the Application Administrator roles.

Type of Administrative Role	**Specific Roles**
Application Administrator	System Administrator
	Password Management Role
	Role Administrator
	Access Request Administrator

Table 5 Administrative Roles

Users with the System Administrator role are authorized to manage all aspects of the TOE including defining and managing identity and credential attributes. The other roles and entitlements provide a subset of administrative functionality as defined in **Table 3**.

6.5 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.

6.5.1 FPT_APW_EXT.1

The following passwords and credentials are stored encrypted using AES in the Oracle database in the operational environment: passwords that are entered in Access Requests (temporarily while being requested); and Administrator credentials. The Administrator credentials are stored for collectors and connectors for accessing the authentication servers and for provisioning purposes. The access request passwords exist for a configurable period of time, with a default of 48 hours and are removed after one view. The encryption keys are stored in the file system and protected by file permissions. The key is unique to each system and there is a user account for the process that owns the key.

All other authentication data is stored by the authentication servers in the Operational Environment. The TOE does not store any enterprise user credentials and does not offer any interfaces to read plaintext passwords.

6.5.2 FPT_SKP_EXT.1

TLS certificates are stored in the server.keystore file in the Oracle database in the environment. An administrator is unable to read or view any keys (stored or ephemeral) through “normal” interfaces.

6.6 TOE Access

RSA Identity Governance and Lifecycle terminates local and remote interactive sessions after an Administrator configurable time period of inactivity; provides users the capability to terminate their own interactive sessions; and displays a configurable advisory warning message regarding unauthorized use of the TOE before establishing a user session using the GUI.

6.6.1 FTA_SSL.3

The TOE terminates remote interactive sessions after an Administrator configurable time period of inactivity (default 10 minutes). The TOE enforces inactive session termination for remote users accessing the TOEs GUI, and for remote Web Service Client Users. The inactive time interval can be set from 5 minutes to 999 minutes.

6.6.2 FTA_SSL.4

The TOE provides both Administrative GUI and Web Services Client users the capability to terminate their own interactive session by logging off. The *logoutUser* call is used to terminate a session with Web Services.

6.6.3 FTA_SSL_EXT.1

The TOE terminates local interactive sessions after an Authorized Administrator specified time period of inactivity (default 10 minutes). The TOE enforces inactive session termination for local users accessing the TOEs GUI. The inactive time interval can be set from 5 minutes to 999 minute.

6.6.4 FTA_TAB.1

The TOE displays a configurable advisory warning message regarding unauthorized use of the TOE before establishing a user session using the GUI.

6.7 Trusted Path/Channels

RSA Identity Governance and Lifecycle uses TLS 1.1 and 1.2 for all communications with trusted external IT entities, and with remote users accessing the TOE via web browser.

6.7.1 FTP_ITC.1

The TOE provides trusted communication channels using TLS v1.1, and TLS v1.2 for the following connections:

- External authentication of users and administrators using AD authentication servers
- Transfer of policy data (includes collection and provisioning)
    - Collection: from Managed Systems to Collectors (local agent)
    - Provisioning: from Connectors (AFX) to Managed Systems

The TOE permits the TSF to initiate communication via the trusted channel.

The TOE relies on FIPS 140-2 validated BSAFE Crypto-J 6.2.1 (CMVP certificate #2468) in the operational environment for cryptographic functions. In particular, the module is used for TLS v1.1 and v1.2 (CVL certificate #471) connections with trusted external IT entities. The TOE supports the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

6.7.2 FPT_TRP.1

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

The TOE requires users to initiate communication via the trusted path for initial user authentication, and execution of management functions.

The TOE relies on FIPS 140-2 validated BSAFE Crypto-J 6.2.1 (CMVP certificate #2468) in the operational environment for cryptographic functions. In particular, the module is used for TLS v1.1 and v1.2 (CVL certificate #471) connections with users accessing the TOE.

7. Protection Profile Claims

This ST is conformant to the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, October 24, 2013 and including the following optional SFRs: FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, and FTA_TAB.1.

As explained in Section 3, Security Problem Definition, the Security Problem Definition of the [ESMICM] has been included in this ST by reference and includes the optional assumptions: A.CRYPTO, A.ROBUST, and A.SYSTIME.

As explained in Section 4, Security Objectives, the Security Objectives of the [ESMICM] have been included by reference and in the case of environmental objectives copied verbatim into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from the [ESMICM]. The only operations performed on the SFRs drawn from the [ESMICM] are assignment and selection operations.

The following table identifies the SFRs that are satisfied by the TOE.

Requirement Class	Requirement Component	Source
ESM: Enterprise Security Management	ESM_EAU.2: Reliance on Enterprise Authentication	ESMICM
	ESM_EID.2: Reliance on Enterprise Identification	ESMICM
	ESM_ICD.1: Identity and Credential Definition	ESMICM
	ESM_ICT.1: Identity and Credential Transmission	ESMICM
FAU: Security audit	FAU_GEN.1: Audit Data Generation	ESMICM
	FAU_STG_EXT.1: External Audit Trail Storage	ESMICM
FIA: Identification and Authentication	FIA_USB.1: User-Subject Binding	ESMICM
FMT: Security management	FMT_MOF.1: Management of Functions Behavior	ESMICM
	FMT_SMF.1: Specification of Management Functions	ESMICM
	FMT_SMR.1: Security Management Roles	ESMICM
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Stored Credentials	ESMICM
	FPT_SKP_EXT.1: Protection of Secret Key Parameters	ESMICM
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination	ESMICM
	FTA_SSL.4: User-initiated Termination	ESMICM
	FTA_SSL_EXT.1: TSF-initiated Session Locking	ESMICM
	FTA_TAB.1: Default TOE Access Banners	ESMICM
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF Trusted Channel	ESMICM
	FTP_TRP.1: Trusted Path	ESMICM

Table 6 SFR Protection Profile Sources

8. Rationale

This security target includes by reference the ESMICM Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the ESMICM assumptions. This security target includes the optional assumptions and objectives from the ESMICM as identified below in the mapping: see **Table 7**. ESMICM security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow ESMICM application notes and assurance activities. Consequently, ESMICM rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

According to Tables 6 and 7 in the ESMICM PP the optional assumptions and objectives map as follows.

Assumptions	Objectives	Rational

A.CRYPTO	OE.CRYPTO	It is expected that vendors will typically rely on the usage of cryptographic primitives implemented in the Operational Environment to perform cryptographic protocols provided by the TOE. If the TOE provides its own cryptographic primitives, then this becomes an objective for the TOE rather than for the environment. The TOE does not rely on its own cryptographic primitives and therefore this objective is appropriate for the TOE.
A.ROBUST	OE.ROBUST	The ESM deployment as a whole is expected to provide a login frustration mechanism that reduces the risk of a brute force authentication attack being used successfully against the TSF and defines allowable conditions for authentication (e.g. day, time, location). It is expected that if the TSF does not provide this mechanism, then it will receive this capability from elsewhere in the ESM deployment. If the ST claims FIA_AFL.1, FIA_SOS.1, and FTA_TSE.1, the ST author must exclude this mapping because robust TOE authentication will be provided by the TSF. The ST does not claim FIA_AFL.1, FIA_SOS.1, or FTA_TSE.1, therefore this objective along with the O.ROBUST satisfy the deployment requirement.
A.SYSTIME	OE.SYSTIME	The TSF is expected to use reliable time data in the creation of its audit records. If the TOE is a software-based product, then it is expected that the TSF will receive this time data from a source within the Operational Environment such as a system clock or NTP server. If the ST claims FPT_STM.1, the ST author must exclude this mapping because system time functionality will be provided by the TSF. The ST does not claim FPT_STM.1. The TOE is software-based product that receives the reliable time data from a source within the Operational Environment.

Table 7: Mapping of optional assumptions and objectives

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 8: Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Enterprise security management	Security audit	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels
ESM_EAU.2	X						
ESM_EID.2	X						
ESM_ICD.1	X						
ESM_ICT.1	X						
FAU_GEN.1		X					
FAU_STG_EXT.1		X					
FIA_USB.1			X				
FMT_MOF.1				X			
FMT_SMF.1				X			
FMT_SMR.1				X			
FPT_APW_EXT.1					X		
FPT_SKP_EXT.1					X		
FTA_SSL.3						X	
FTA_SSL.4						X	
FTA_SSL_EXT.1						X	
FTA_TAB.1						X	
FTP_ITC.1							X
FTP_TRP.1							X

Table 8: Security Functions vs. Requirements Mapping