National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Information Security Corporation CertAgent v7.0 Patch Level 9

Report Number: CCEVS-VR-VID11180-2021
Dated: 08/06/2021
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
Attn: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

<u>Validation Team</u>

Aerospace Corporation

Ken Elliott

Meredith Hennan

Swapna Katikaneni

Seada Mohammed

<u>Common Criteria Testing Laboratory</u>

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Information Security Corporation CertAgent v7.0 patch level 9 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR 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 Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos. The evaluation determined that the TOE is:

- Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant

and demonstrates exact conformance to:

- *Protection Profile for Certification Authorities,* version 2.1 2017-12-01 ([5])

as clarified by all applicable Technical Decisions.

The TOE is Information Security Corporation CertAgent Version 7.0 patch level 9 for Windows and Information Security Corporation CertAgent Version 7.0 patch level 9 for Linux.

The TOE identified in this VR has been evaluated at a NIAP approved and NVLAP accredited CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

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

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST ([6]).

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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).

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

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	• CertAgent Version 7.0 patch level 9 for Windows • CertAgent Version 7.0 patch level 9 for Linux
Security Target	ISC CertAgent v7.0 patch level 9 Security Target for Common Criteria Evaluation, Software Version: 7.0 patch level 9, Document Version: 4.2.9, Issue Date: July 27, 2021
Sponsor & Developer	Information Security Corporation 1011 W. Lake St., Ste. 425 Oak Park, IL 60301 www.infoseccorp.com
Completion Date	August 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	Protection Profile for Certification Authorities, version 2.1 2017-12-01
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant

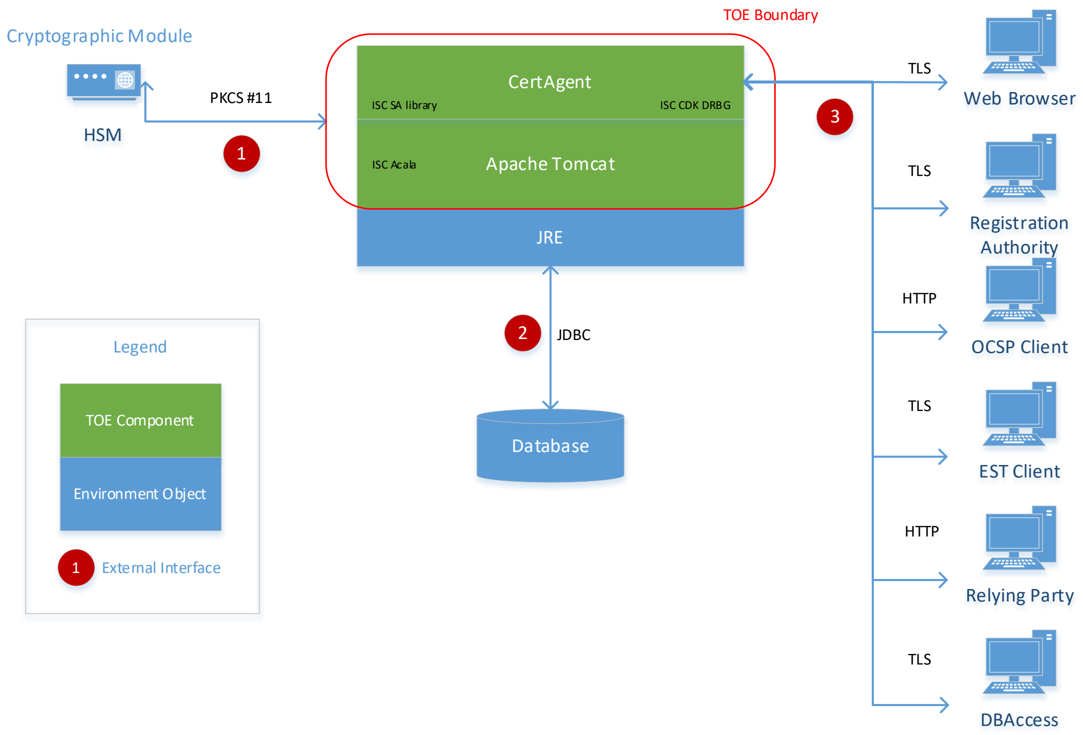
Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Furukh Siddique Greg Beaver Pascal Patin
Validation Personnel	*Aerospace Corporation* Ken Elliott Meredith Hennan Swapna Katikaneni Seada Mohammed

3 TOE Architecture

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

CertAgent, the TOE, is an X.509-compliant certificate authority (CA). It is a web-based certificate authority (CA) intended to be used as the core component of an enterprise public key infrastructure (PKI). Designed to meet the needs of a wide variety of organizations, the current release offers enhanced enrollment services (EST), remote administration, integrated certificate and CRL database, and an OCSP responder. It supports an unlimited number of root and intermediate CAs, providing support for as complex a certificate hierarchy as the size of the enterprise warrants. The following diagrams shows the TOE boundary and major components.

Figure 1 Information Security Corporation CertAgent v7.0 patch level 9 TOE Boundary



As Figure 1 shows, CertAgent combined with Apache Tomcat form the Target of Evaluation (TOE). There are 4 high level interfaces that are external to the TOE. The data that traverses these interfaces is protected as shown in the following table.

Interface	Protection
Web	HTTP, HTTPS/TLS
Database	Operating system
OCSP	HTTP, HTTPS/TLS

PKCS#11	Operating system

Most CA activities are completed by using a web browser or other tool that connects to the CertAgent web interface. The CA supports seven web-based interfaces using different ports or URLs (Admin Site, CA Account Site, Public Site, RAMI (Registration Authority Management Interface), DBAccess, EST, and OCSP).

- The Admin Site, CA Account Site, DBAccess, and Registration Authority (RAMI) channels require valid identification and authentication credentials in the form of certificates. This channel is secured using client authenticated HTTPS/TLS.
- The Public Site channel is secured using HTTPS/TLS and HTTP. All pages except the CA Information page are HTTPS/TLS protected. The CA information page, used by relying parties to obtain CRLs, issuer certificates, and CA version information, is available without security over HTTP. All pages except the self-service revocation page are unauthenticated. The self-service revocation page requires valid identification and authentication credentials in the form of certificates.
- The EST channel is secured using HTTPS/TLS. Connections are authenticated with either certificates or a subscriber name and password.
- The OCSP interface is available without security over HTTP or secured using HTTPS/TLS. All access is unauthenticated.

Configuration data (including ACLs), most audit logs, certificates, and CRLs are stored in tables in a single database. In the evaluated configurations, the database is either HyperSQL or PostgreSQL and is hosted on the same physical system as the TOE. The connection to the database is not secured but is authenticated. Sensitive data stored in the database is encrypted before it is sent to the database for storage. The environmental JRE's JDBC API is used to communicate with the database using a database vendor supplied JDBC driver.

CertAgent has an option to connect to LDAP servers to push certificate and CRLs as they are issued. Since certificates and CRLs are public information this connection may be unsecure or secure and may or may not be authenticated. There is no LDAP server in the evaluated configuration, LDAP publishing was not evaluated, and LDAP publishing is disabled when CertAgent is configured with strict NIAP compliance settings.

CertAgent's OCSP capability is divided into basic OCSP support and enhanced OCSP support. Basic OCSP support provides OCSP responses for issuers managed by the CertAgent instance. If enabled, enhanced OCSP support, known as Dhuma, provides OCSP responses for issuers not managed by the CertAgent instance. The evaluated configuration enabled enhanced OCSP support but operating the TOE with basic OCSP support is considered equivalent.

Private keys used for issuing certificates, issuing CRLs, authenticating the TLS server, and signing OCSP responses reside in the environmental PKCS#11 Cryptographic Module. In the evaluated configuration, the PKCS#11 Cryptographic Module, is a Thales Luna USB HSM[1], but any PKCS#11 Cryptographic Module that is at least FIPS 140-2 Level 2 validated, provides hardware security of keys, includes a PKCS#11 library,

[1] This is the current trade name of the device. The device used in the evaluation is branded as Gemalto SafeNet USB HSM as it was produced prior to the Thales acquisition of Gemalto. The device uses the Luna G5 Cryptographic Module with FIPS 140-2 certificate #3210, password authentication, and supports cloning the device for backup purposes (G5 PW-AUTH CL).

supports the required algorithms (in particular a 256-bit DRBG with 256-bits of entropy input), and provides a backup capability, is considered equivalent. PKCS#11 is a C API exported from a shared library (a DLL or .so depending on platform that is provided by the HSM vendor). The TOE loads this library on startup and calls functions in it as it would any other local library. Data traversing this interface is protected by the environmental operating system in which processes are segregated into their own process space and are logically separated from all other processes by the operating system and underlying hardware.

4 Security Policy

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

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Security Audit

The TOE generates audit records of administrator, user, and its own activities. Audit data includes date, time, event type, subject identity, and other data as required. Most audit data are written to the database. Audit records indicating a database failure are stored in a local text file as the database is inaccessible. The TOE allows an external IT entity to access TOE audit records in the database by polling the TOE using the DBAccess REST API.

4.2 Communications

The TOE relies on the TLS/HyperText Transfer Protocol Secure (HTTPS) when transmitting sensitive data to and from applicable endpoints.

Certificate requests, certificates, CRLs, and OCSP responses are formed and verified according to RFC 5280, RFC 6960, and RFC 7030. Certificate validation is performed by the TOE.

Sensitive data that needs to be recovered (PKCS#11 Cryptographic Module PINs and other authentication passwords) are encrypted using CMS, in conformance with RFC 5652, and then stored in the database. Sensitive data that does not need to be recovered, EST passwords, are not stored directly, but a check value is created, using PBKDF2/SHA-256, and stored.

4.3 Cryptographic Support

Cryptographic support is provided by two components.

- ISC's Cryptographic Development Kit (ISC CDK)
- PKCS#11 Cryptographic Module

ISC CDK

The ISC CDK is within the TOE's boundary and is used by the TOE:

- to generate the initial set of authentication credentials (certificates and associated private keys) during installation,
- to generate symmetric keys, wrap them with public keys, and use them to encrypt sensitive data using the CMS format,
- to hash the "to be signed" message bodies of certificates, CRLs, and OCSP responses
- to validate signatures on certificates, CRLs, and requests, and
- to provide communication protection when clients establish TLS/HTTPS connections to the Administrative, CA, Public, EST, OCSP, DBAccess, or RAMI interfaces. Note: Cryptographic functions involving the TLS server private key are provided by the environmental PKCS#11 Cryptographic Module.

PKCS#11 Cryptographic Module

The PKCS#11 Cryptographic Module is used by the TOE:

- to generate, store, and provide cryptographic operations (unwrapping DEKs) involving the private key for the "System" credential (certificate and private key),
- to generate, store, and provide cryptographic operations (digital signatures) involving the private key for all issuer credentials (certificates and private keys), and
- to generate, store, and provide cryptographic operations (digital signature) involving the private key for the TLS/HTTPS server credential (certificate and private key).

The PKCS#11 Cryptographic Module securely stores the high value certificate authority keys and uses them to perform the signature operations that define a certificate authority. The PKCS#11 Cryptographic Module also securely stores the TLS/HTTPS server key and provides cryptographic services involving that key. PKCS#11 Cryptographic Modules often require a PIN or other authentication when the application using them starts and the TOE provides mechanisms for injecting this information during its startup procedures.

In the evaluated configuration, the PKCS#11Cryptographic Module is Thales' Luna USB HSM

4.4 User Data Protection

The TOE supports the creation of multiple certificate profiles by CA Administrators. Each profile is customizable by a CA Administrator and includes a certificate-based ACL of CA Operations Staff members allowed to issue or revoke certificates using the profile. Certificate requests are assigned a unique identifier upon submission that is used to link the request to the issued certificate.

The TOE provides relying parties two methods to check the status of a certificate:

- X.509v2 CRLs
- OCSP

CRLs can be issued manually, on a schedule, or when a certificate is revoked for a set of configurable reason codes.

4.5 Identification and Authentication

The TOE uses two different identification and authentication methods, depending on the role and action being performed:

- EST authentication - EST authentication supports either certificate-based authentication or subscriber name/password authentication (over HTTPS) in cases where the requester does not have a valid certificate. For subscriber name/password authentication (over HTTPS), privileged users in the CA Operation Staff role create and manage the subscriber name/password associations.
- Certificate-based Identification and Authentication - Access to the Admin Site, CA Account Site, DBAccess API, or RAMI API requires certificate-based client authentication using HTTPS. The functions available depend on the ACL and permissions that are assigned to the certificate used to authenticate. The portion of the Public Site allowing self-service revocation by subscribers also requires certificate-based client authentication using HTTPS.

Most TOE activities, and all activities involving the issuance or revocation of certificates, require certificate-based authentication.

PKCS#11 Cryptographic Modules support a variety of authentication options including passwords, smart cards, PED devices, and fingerprints. In all cases, someone must enable the PKCS#11 Cryptographic Module as part of the initialization of the TOE. This step is performed locally on the system during startup of the TOE.

Access to the TOE's local console is controlled by the underlying environmental operating system which performs the required identification and authentication when an administrator logs on.

4.6 Security Management

The TOE is managed by authorized administrators using a web user interface and the local console as needed. All certificate issuance related administrative actions are performed via the web interface. The TOE supports three (3) roles (Administrator, Auditor, and CA Operations Staff) each of which consists of an access control list (ACL) of one or more X.509 certificates and one or more permissions (issue, revoke, RAMI, etc.).

Only users who hold an administrator role in the TOE are allowed to have administrator privileges on the physical system on which the TOE is installed. They can:

- inject the PKCS#11 Cryptographic Module PIN to unlock the "System" credential's private key,
- start/stop the TOE and the Database,
- run the CACLI program (allows the scripting of the creation of a root or issuer, trust anchor management, ACL management),
- run the Report Generator Program, or
- run the update tool (to check for updates or apply updates to the system).

4.7 Protection of the TSF

The TOE encrypts any sensitive information, before it is sent to the environmental database, using the asymmetric "System" credential's public key and the CMS format. These encrypted symmetric keys are the only symmetric keys that are persisted by the TOE. When the information is needed later, the encrypted data is retrieved from the database, and the TOE uses the "System" credential's private key, via the PKCS#11 Cryptographic Module's PKCS#11 API, to unwrap the symmetric key.

The TOE maintains the password of PKCS#11 Cryptographic Module storing the "System" credential in memory until it exits. The TOE does not store, or directly use, any private keys (they are stored and protected by the PKCS#11 Cryptographic Module which performs operations with those keys at the TOE's request). When the TOE shuts down all sensitive data in memory is cleared.

4.8 TOE Access

The TOE's Admin Site and CA Account Site display a warning banner prior to allowing any administrative actions to be performed. The TOE's web interface will terminate sessions when they time out or when an authenticated user clicks the logout link in the navigation pane.

4.9 Trusted Path/Channels

The TOE provides a trusted path/channel for secure communication between itself and external IT entities such as a registration authority (RA), audit server, or similar entities which are permitted to connect to the TOE, over client authenticated HTTPS/TLS. Privileged users accessing the TOE's web interfaces also use a trusted path established and secured with client authenticated HTTPS/TLS.

Subscribers with existing, valid certificates, also use a trusted path, established and secured with client authenticated HTTPS/TLS, to perform certificate renewal, via EST, or self-management, via the TOE's Public Site web interface. Subscribers, and other non-privileged users, are permitted to connect to the TOE's Public Site with unauthenticated HTTPS/TLS. Relying parties are permitted to connect to parts of the TOE's Public Site, with either unauthenticated HTTPS/TLS or unprotected HTTP, to obtain certificate status or other information required to validate certificates issued by the TOE.

For communication between the TOE and environmental components (notably the database and the HSM) the Operational Environment provides a non-encrypted, trusted channel. Secure communication is enforced between the TOE and IT entities in the Operational Environment using the Operational Environment's JRE, JNDI, JDBC, and PKCS #11 Cryptographic Module components installed on the local system. These trusted channels transfer TOE data to and from IT entities within the Operational Environment.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5.2 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in *Protection Profile for Certification Authorities,* version 2.1 2017-12-01 ([5]) and performed by the evaluation team).
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The TOE does not include the operating systems or hardware of the systems on which it is installed. It also does not include the third-party software required for the TOE to run. **Error! Reference source not found.** below list the software components required by the TOE in the evaluated configurations. The Operational Environment components should be maintained such that the latest security fixes for each component are installed in a timely manner.

Component	Requirement
Server OS	Windows Server 2016
OS Type	64-bit
Database	HyperSQL Version 2.5.1
Java JRE	Oracle Java 11.0.8
PKCS#11 Cryptographic Module	Thales Luna USB HSM model G5 PW-AUTH CL; firmware version 6.24.7

Operational Environment Software Requirements (Windows)

Component	Requirement

Server OS	CentOS 7.8 w/rng-tools package
OS Type	x86_64 (64-bit)
Database	PostgreSQL Version 11.9
Java JRE	Oracle Java 11.0.8
PKCS#11 Cryptographic Module	Thales Luna USB HSM model G5 PW-AUTH CL; firmware version 6.24.7

Operational Environment Software Requirements (Linux)

- The evaluation of security functionality of the product was limited to the functionality specified in *ISC CertAgent v7.0 patch level 9 Security Target for Common Criteria Evaluation*, Software Version: 7.0 patch level 9, Document Version: 4.2.9, Issue Date: July 27, 2021 ([6]).
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in [6].
- 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.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *CertAgent Guidance for Common Criteria Evaluation Software Version: 7.0 patch level 9, Document Version: 2.6.3* ([7])

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

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

- *CertAgent 7.0 Common Criteria Test Report and Procedures For Protection Profile for Certification Authorities Version 2.1, Version 1.2, Dated: July 28, 2021* ([10])

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Information Security Corporation CertAgent v7.0 Patch Level 9, Version 1.1, July 28, 2021* ([9])

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *Protection Profile for Certification Authorities* ([5]).

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Certification Authorities* ([5)]. 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 Leidos CCTL facilities in Columbia, Maryland, from January 2021 through August 5, 2021.

The evaluators received the TOE in the form that 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.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Certification Authorities* were fulfilled.

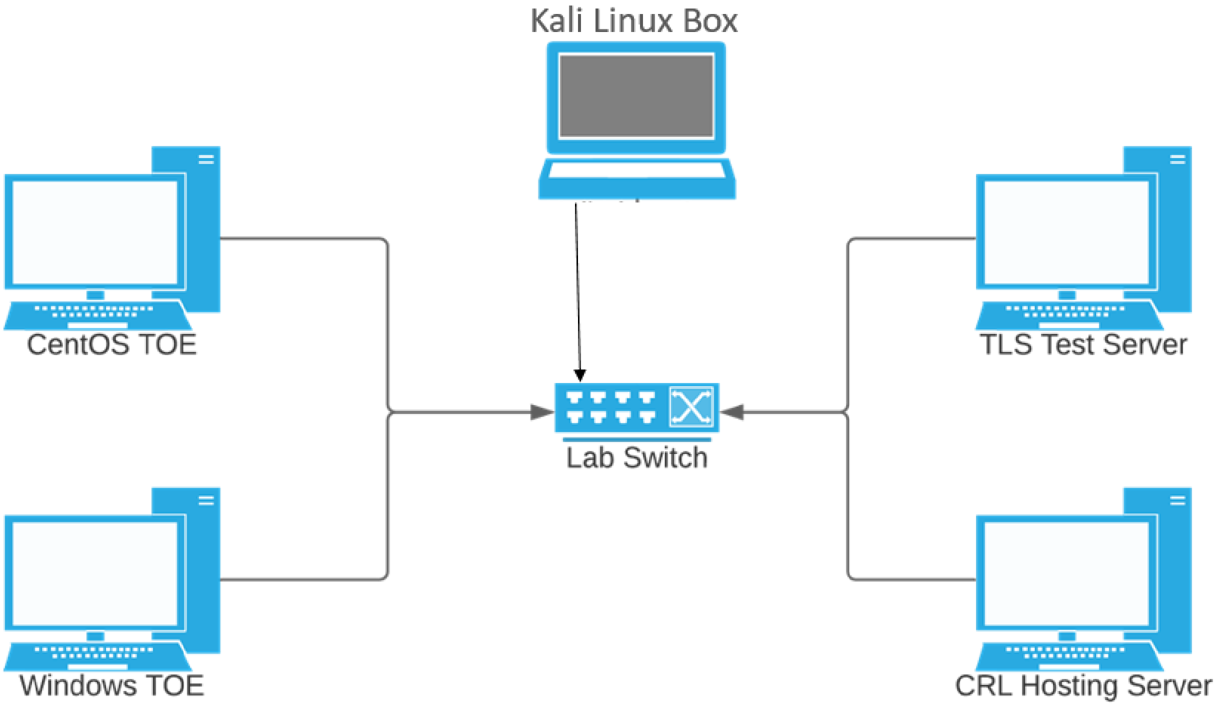
7.1 Test Configuration

The evaluation team established a test configuration consisting of the Information Security Corporation CertAgent Version 7.0 patch level 9 for Windows and Information Security Corporation CertAgent Version 7.0 patch level 9 for Linux the installed on each of the following devices:

- The Windows Server version of the TOE was evaluated on a Dell Inspiron 5593 laptop with an Intel Core i7-1065G7 CPU based on the Intel Ice Lake microarchitecture.

- The CentOS version of the TOE was evaluated on a Dell XPS 15 9560 laptop with an Intel Core i7-7700HQ CPU based on the Intel Kaby Lake microarchitecture.

The following components were used to create the test configuration:



- CentOS TOE
  - CentOS Linux 7 with Linux 3.10.0 x86_64 kernel
  - Intel Core i7-7700HQ CPU
- Windows TOE
  - Windows Server 2016 Standard
  - Inter Core i7-1065G7 CPU
- TLS Test Server
  - Ubuntu 18.04
  - OpenSSL 1.1.1
  - Custom Lab TLS Server and Client test tools
- CRL Hosting Server
  - Ubuntu 18.04
- Kali Linux Box
  - Kali Linux Release 2020.4
  - Curl 7.72.0 (used as EST client)
  - Wireshark 2.6.10
  - XCA Certificate Authority 2.0.1

- OpenSSL 1.1.1
- SSLyze 2.1.4 SSL/TLS Testing Tool

8 Evaluated Configuration

The evaluation team established a test configuration consisting of the Information Security Corporation CertAgent Version 7.0 patch level 9 for Windows and Information Security Corporation CertAgent Version 7.0 patch level 9 for Linux installed on the following devices:

- The Windows Server version of the TOE was evaluated on a Dell Inspiron 5593 laptop with an Intel Core i7-1065G7 CPU based on the Intel Ice Lake microarchitecture.
- The CentOS version of the TOE was evaluated on a Dell XPS 15 9560 laptop with an Intel Core i7-7700HQ CPU based on the Intel Kaby Lake microarchitecture.

The TOE requires the use of a Thales Luna USB HSM external PKCS#11 Cryptographic Module

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report For Information Security Corporation's CertAgent Version 7.0 Patch Level 9 Part 2 (Proprietary), ([9]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in *Protection Profile for Certification Authorities, version 2.1 2017-12-01* ([5]). The evaluation determined the TOE satisfies the conformance claims made in the *ISC CertAgent v7.0 patch level 9 Security Target for Common Criteria Evaluation*, Software Version: 7.0 patch level 9 of Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in:

- *Protection Profile for Certification Authorities, version 2.1, 2017-12-01* ([5]).

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed Protection Profile, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV assurance activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance assurance activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed Protection Profile. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

Searches of public vulnerability repositories were performed on July 28, 2021.

The evaluation team searched the following public vulnerability repositories.

- National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search).

The evaluation team used the following search terms in the searches of these repositories:

- Information Security Corporation
- ISC
- CertAgent version 7
- CertAgent
- ISC Acala
- ISC SA Library
- ISC CDK DRBG
- ISC CDK
- Apache Tomcat
- HyperSQL
- PostgreSQL.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed Protection Profile. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

All of the validators' comments are covered in the *Clarification of Scope* section (5.2) of this report. There are no additional validator comments or recommendations.

11 Security Target

The ST for this product's evaluation *is ISC CertAgent v7.0 patch level 9 Security Target for Common Criteria Evaluation*, Software Version: 7.0 patch level 9, Document Version: 4.2.9, Issue Date: July 27, 2021 [6].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PII	Personally Identifiable Information
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VMI	Virtual Mobile Infrastructure
VR	Validation Report

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Certification Authorities, version 2.1, 2017-12-01.

[6] ISC CertAgent v7.0 patch level 9 Security Target for Common Criteria Evaluation, Software Version: 7.0 patch level 9, Document Version: 4.2.9, Issue Date: July 27, 2021.

[7] CertAgent Guidance for Common Criteria Evaluation Software Version: 7.0 patch level 9, Document Version: 2.6.3, Issue Date: July 27, 2021

[8] Evaluation Technical Report For Information Security Corporation's CertAgent Version 7.0 Patch Level 9 Part 2 (Proprietary), Version 1.1, 28 July 2021.

[9] Assurance Activities Report for Information Security Corporation CertAgent v7.0 Patch Level 9, Version 1.1, July 28, 2021.

[10] CertAgent 7.0 Common Criteria Test Report and Procedures For Protection Profile for Certification Authorities Version 2.1, Version 1.2, Dated: July 28, 2021.