National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Information Security Corporation (ISC) CertAgent v 7.0

Report Number: CCEVS-VR-10815-2018

Dated: 1 June 2018

Version: 1.0

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

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Ken Elliott, Senior Validator

Chris Thorpe, Lead Validator

Lisa Mitchell, ECR Team

Jennifer Dotson, ECR Team

Evaluation Team

Eve Pierre

Michael Esposito

Common Criteria Testing Laboratory

DXC
10830 Guilford Road, Suite 307
Annapolis Junction, Maryland 20701

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. For more detailed information on how the product was assessed, the end-users should review the Assurance Activity Report (AAR). 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.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of ISC CertAgentv7.0, the Target of Evaluation (TOE), performed by DXC. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was performed by DXC of Annapolis Junction, MD in accordance with the United States evaluation scheme and completed in July 2018. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The evaluation was conducted in accordance with the requirements of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, dated April 2017, the *Common Evaluation Methodology for IT Security Evaluation (CEM)*, Version 3.1, Revision 5, April 2017, and assurance activities specified in *Protection Profile for Certification Authorities*, version 2.1, 1 December 2017.

The DXC evaluation team determined that ISC CertAgentv7.0 is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST.

ISC CertAgent v7.0, the TOE, is an X.509-compliant web-based certificate authority (CA) intended to be used as the core component of an enterprise public key infrastructure (PKI). The TOE offers enhanced enrollment services via Enrollment over Secure Transport (EST), remote administration, integrated certificate and certificate revocation list (CRL) databases, and an online certificate status protocol (OCSP) responder. It supports an unlimited number of root and intermediate CAs, providing support for complex certificate hierarchies.

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

and assurance requirements stated in the ST. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

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 Validated Products List.

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	ISC CertAgent v7.0
Protection Profile	Protection Profile for Certificate Authorities, version 2.1, 2017-12-01
Security Target	CertAgent Security Target for Common Criteria Evaluation, version 4.1.1, 07/11/2018
Dates of evaluation	December 4, 2017 – July 17, 2018
Assurance Activity Report	Assurance Activity Report for CertAgent version 7.0, Document version 1.5a, July 17, 2018
Evaluation Technical Report	Evaluation Technical Report for ISC CertAgent version 7.0, Document version 1.0, July 17, 2018
Conformance Result	CC Part 2 extended and CC Part 3 conformant
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 5, April 2017
Common Evaluation Methodology (CEM) version	CEM version 3.1R5, April 2017
Sponsor	Information Security Corporation (ISC)
Developer	Information Security Corporation (ISC)
Evaluators	Eve Pierre, Michael Esposito
Validation Team	Kenneth Elliott, Chris Thorpe, Lisa Mitchell, Jennifer Dotson

3. SECURITY POLICY

The TOE is intended to be used in a range of security settings (i.e., computers coupled to a single TOE can vary from non-classified Internet connected to those protected in accordance with national security policy). Any data leakage across the TOE may cause severe damage to the organization and therefore must be prevented.

4. SECURITY PROBLEM DEFINITION

Assumptions

The ST identified the following security assumptions:

TABLE 1: TOE ASSUMPTIONS

Assumption Name	Assumption Definition
A.NO_GENERAL_PURPOSE	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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

Threats

The ST identified the following threats addressed by the TOE:

TABLE 2: TOE THREATS

Threat Name	Threat Definition
T.PRIVILEGED_USER_ERROR	A privileged user or non-person entity (NPE) improperly exercises or adversely affects the TOE, resulting in unauthorized services, ineffective security mechanisms, or unintended circumvention of security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHENTICATED_TRANSACTIONS	Relying parties within an information system depend on the TOE to accurately bind subjects to their credentials for use in authenticating and providing privacy for transactions. Without the proper binding provided by the TOE, relying parties cannot ensure adequate access controls on sensitive information, ensure transactional integrity, ensure proper accountability, and/or enforce non-repudiation.
T.UNAUTHORIZED_ACCESS	A malicious user, process, or external IT entity intentionally circumvents TOE security mechanisms.

T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNDETECTED_ACTIONS	Remote users or external IT entities may take actions that adversely affect the security of the TOE.
T.USER_DATA_REUSE	A malicious user, process, or external IT entity may gain access to user data that is not cleared when resources are reallocated.
T.WEAK_CRYPTO	A weak hash or signature scheme may be compromised by an attacker and used to apply integrity checks to malicious content so that it appears legitimate.

Organizational Security Policies

The Security Target identifies the following Organizational Security Policies (OSPs) to which the TOE must comply.

TABLE 3: ORGANIZATIONAL SECURITY POLICIES

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

5. ARCHITECTURAL INFORMATION

Physical Scope and Boundary

CertAgent, the TOE, is an X.509-compliant web-based certificate authority (CA) intended to be used as the core component of an enterprise public key infrastructure (PKI). The TOE 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 diagram shows the TOE boundary and major components.

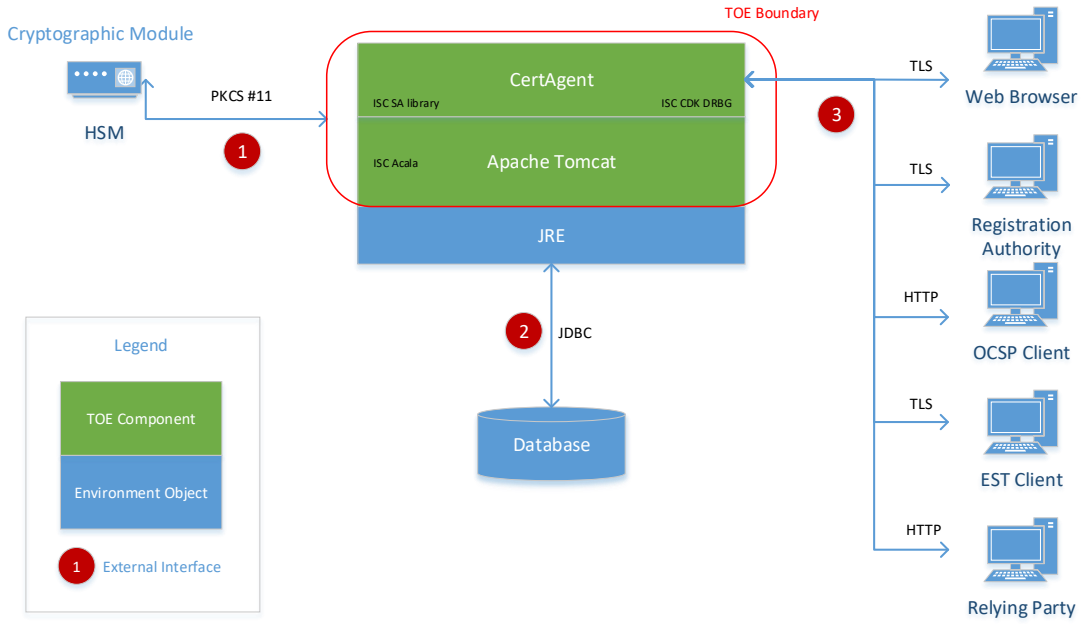

FIGURE 1 TOE BOUNDARY

The physical boundary of the TOE includes the ISC CertAgent v7.0 software, installed on a general-purpose computer, running a supported operating system. The TOE software includes the following components:

- CertAgent 7.0.6 — The certification authority software web application.
- Apache Tomcat — Apache Tomcat application server that hosts the CertAgent web app and the web interface. In the evaluated configuration Apache Tomcat is configured to use the ISC CDK and the PKCS#11 Cryptographic Module for cryptographic operations.

- ISC CDK — The cryptographic module in the TOE.

The TOE does not include the hardware, database, HSM, or the operating systems of the computers on which it is installed. It also does not include third-party software required for the TOE to run.

Components and Applications Required in the TOE Operational Environment
The TOE operates with the following components in its operational environment:

- Server OS – The OS platforms that host the TOE.
- Database — installed on the TOE host platform, the database is used to store the TOE configuration data (including ACLs), audit logs, certificates, and CRLs for the TOE.
- Java JRE — Runs the CertAgent and application servers.
- JCE Unlimited Strength Jurisdiction Policy — Enables unlimited strength cryptography in Java which is required to support the AES-256 ciphersuite.
- PKCS#11 Cryptographic Module — USB HSM connected to the to the same host as the TOE. It stores the private keys used to sign certificates, issue CRLs, create OCSP responses, and authenticate the server to clients via TLS/HTTPS.
- Web Browser — Firefox - installed on client systems and used to access the TOE external interfaces.

The TOE evaluated configuration requires the following on the Windows platform:

- Windows Server 2012 R2
- HyperSQL Version 2.4
- Oracle Java JRE 8 1.8
- Gemalto SafeNet USB HSM

The TOE evaluated configuration requires the following on the Linux platform:

- CentOS 6.7 w/rng-tools package
- PostgreSQL Version 9.4
- Oracle Java JRE 8 1.8

- Gemalto SafeNet USB HSM

Logical Scope and Boundary

The logical scope of the TOE comprises the following security functions:

- Security Audit – The TOE generates audit records of administrator, user and its own actions. The TOE stores its audit trail on the database in the operational environment. The TOE also relies on the underlying operating system to generate and manage some required audit events.
- Communication – The TOE uses TLS/HTTPS when transmitting sensitive data to and from applicable endpoints. Certificate requests, certificates, CRLs and OCSP responses are formed and verified by the TOE. TOE sensitive data that needs to be recovered such as PINs and other passwords are encrypted using CMS before they are stored in the database; sensitive data that does not need to be recovered such as EST passwords are not stored, but a check value is created using PBKDF2/SHA-256 and stored.
- Cryptographic Support – The TOE uses its included ISC CDK cryptographic module 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 TLS/HTTPS secure communication when clients access the TOE interfaces.

  The TOE uses the PKCS#11 cryptographic module in the operational environment to securely store the high value certificate authority keys, to securely store the TLS server key, and to provide cryptographic services involving those keys. In the evaluated configuration, the PKCS#11 cryptographic module is Gemalto's Safenet USB HSM.

- User Data Protection – The TOE supports the creation of multiple certificate profiles by CA Administrators. These profiles are customized using certificate-based ACLs to control the users allowed to issue or revoke certificates using the profiles. Certificate requests are assigned a unique identifier upon submission that links them to the issued certificate. The TOE supports two methods for certificate status checking: X.509v2 CRLs and OCSP. CRLs can be issued manually, on a schedule, or when a certificate is revoked for a set of configurable reason codes.
- Identification and Authentication – The TOE supports EST authentication with either certificate-based authentication or common name/password (over HTTPS).

The TOE implements certificate-based client authentication using HTTPS at its admin, CA, DBAccess and RAMI interfaces.

- Security Management – The TOE provides a web user interface to manage its functions and data and it restricts access to this interface based on user role. The TOE also depends on the underlying OS to provide the local console for managing the TOE. Access to the local console interface is managed by the underlying OS and is restricted to authorized administrators and auditors.
- Protection of the TSF – The TOE encrypts any sensitive information before it is sent to the operational environment's database. The TOE maintains the PKCS#11 cryptographic module password for the 'system' credential in memory until it exits. The TOE does not store any private keys (they are stored and protected by the PKCS#11 cryptographic module). When the TOE shuts down, all sensitive data in memory is cleared.
- TOE Access – The TOE displays a warning banner prior to login at its user interfaces. The TOE's web interface will terminate a session when it times out or when the authenticated user clicks the logout button.
- Trusted Channel/Trusted Path — The TOE provides a trusted path for remote users to access its user interfaces using HTTPS. The TOE also provides a trusted channel between itself and trusted IT entity using TLS/HTTPS.

6. DOCUMENTATION

The TOE includes the following guidance documents:

- CertAgent Administrator Guide, version 7.0, July 5, 2018
- CertAgent Installation, Configuration and Management Guide, version 7.0, July 5, 2018
- CertAgent Certificate Authority Guide, version 7.0, July 5, 2018
- CertAgent Public Site Guide, version 7.0, July 5, 2018
- CertAgent Guidance for Common Criteria Evaluation, version 2.3.0, July 7, 2018
- CertAgent 7.0.6 Release Notes, June 26, 2018

All documentation delivered with the product is relevant to and within the scope of the TOE.

7. IT PRODUCT TESTING

This section describes the testing efforts of the evaluation team.

Evaluation team independent testing

The evaluation team conducted independent testing at the ISC facilities in Oak Park, Illinois. The evaluation team configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Protection Profile test procedures as a basis for creating each of the Independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

8. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.

DXC has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Protection Profile for Certification Authorities, version 2.1, dated December 1, 2017. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was completed in July 2018.

9. VALIDATOR COMMENTS

The functionality evaluated is scoped exclusively to the security functional requirements (SFRs) specified in the Security Target, and only the functionality implemented by the SFRs within the Security Target was evaluated. All other functionality provided by CertAgent v7.0 that are outside the scope of Protection Profile for Certificate Authorities (CAPP) v2.1 are not covered by this evaluation, need to be assessed separately, and no further conclusions can be drawn about their effectiveness.

The validation team notes that the TOE performs two path validation operations to verify the authenticity and trust of a client's certificate. The first path validation is performed by the Apache Tomcat portion of the TOE; this path validation terminates to trust anchors residing in the Apache Tomcat trust store. The second path validation is performed by the CertAgent TOE component on the certificate already verified by Apache Tomcat. This path validation is done using CertAgent's path building and validation processing; CertAgent maintains its own trust anchor list stored in the database.

The TOE consists of a Tomcat applet (and the associated Tomcat implementation) that has significant operational dependencies on its IT environment. Users should ensure that components (hardware, OS, etc.) used to host the TOE have trust that is commensurate with that of the TOE.

10. ANNEXES

Not applicable.

11. SECURITY TARGET

Information Security Corporation CertAgent Security Target for Common Criteria Evaluation, version 4.1.1, July 11, 2018.

12. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 5, April 2017.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 5, April 2017.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 5, April 2017.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 5, April 2017.
5. Information Security Corporation CertAgent Security Target for Common Criteria Evaluation, version 4.1.1, July 11, 2018.
6. Assurance Activity Report for CertAgent v7.0, document version 1.5a, July 17, 2018.
7. Evaluation Technical Report for ISC CertAgent Version 7.0, document version 1.0, July 17, 2018.
8. CertAgent 7.0 Detailed Test Report, document version 2.3, July 17, 2018.
9. CertAgent Guidance for Common Criteria Evaluation, document version 2.3.0, July 7, 2018.