National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Protection Profile for Certification Authorities

Version 2.1

01 December 2017

Report Number: CCEVS-VR-PP-0052
Dated: 09 September 2019
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
DXC Security Testing/Certification Laboratories
Annapolis Junction, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for Certification Authorities, Version 2.1, (PP_CA_V2.1) [6]. It presents a summary of the PP_CA_V2.1 and the evaluation results.

DXC Security Testing/Certification Laboratories, located in Annapolis Junction, Maryland, performed the evaluation of PP_CA_V2.1 concurrent with the first product evaluation against the PP's requirements. The evaluated product was CertAgent Version 7.0.

This evaluation addressed the base requirements of PP_CA_V2.1 and several of the additional requirements contained in Appendices A, B and C.

The Validation Report (VR) author independently performed an additional review of the PP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements.

The evaluation determined that PP_CA_V2.1 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this VR has been evaluated at NIAP approved CCTLs 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). Because the CertAgent Security Target contains only material drawn directly from PP_CA_V2.1, the majority of the ASE work units served to satisfy the APE work units as well.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against PPs that contain Evaluation Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of PP_CA_V2.1 was performed concurrent with the first product evaluation against the PP's requirements. In this case, the Target of Evaluation (TOE) was CertAgent Version 7.0, evaluated by DXC Security Testing/Certification Laboratories in Annapolis Junction, Maryland, United States of America

These evaluations addressed the base requirements of PP_CA_V2.1, and several of the additional requirements contained in Appendices A, B and C.

PP_CA_V2.1 contains a set of "base" requirements that all conformant STs must include, and additionally contains "Optional", "Selection-based", and "Objective" requirements. Optional requirements may or may not be included within the scope of the evaluation,

depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE. Objective requirements specify optional functionality that the PP authors consider candidates for becoming mandatory requirements in the future.

A specific ST may not include all non-base requirements, so the initial use of the PP addresses (in terms of the PP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ workunits performed against PP_CA_V2.1. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of PP_CA_V2.1 were evaluated.

The following identifies the PP subject of the evaluation/validation, as well as the supporting information from the evaluation performed against this PP and any subsequent evaluations that address additional optional and/or selection-based requirements in the PP_CA_V2.1.

Protection Profile	Protection Profile for Certification Authorities, Version 2.1, 01 December 2017.
ST (Base)	CertAgent Security Target for Common Criteria Evaluation, Software Version 7.0, Document Version 4.1.1, 11 July 2018.
Assurance Activity Report (Base)	Assurance Activity Report For CertAgent Version 7.0, Document version: 1.5a, 07 July 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTLs	DXC Security Testing/Certification Laboratories, Annapolis Junction, Maryland

3 PP_CA_V2.1 Description

The PP_CA_V2.1 specifies information security requirements for certification authorities, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

This Protection Profile (PP) describes security requirements for a Certification Authority is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well-defined and described threats. These requirements support CA operations performed in accordance with the National Institute of Standards and Technologies (NIST) Interagency or Internal Report (IR) 7924 (Second Draft), Reference Certificate Policy, May 2014, referred to as the "NIST IR." Terms.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the

development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: 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 assumed to follow and apply all administrator guidance in a trusted manner.

4.2 Threats

The following table contains applicable threats.

Table 2: 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.

4.3 Organizational Security Policies

The following table contains applicable organizational security policies.

Table 3: Organizational Security Policies

OSP Name	OSP 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.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.AUDIT_LOSS_RESPONSE	The TOE will respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.
O.AUDIT_PROTECTION	The TOE will protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.
O.CERTIFICATES	The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.
O.CONFIGURATION_MANAGEMENT	The TOE will conduct configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.INTEGRITY_PROTECTION	The TOE will provide appropriate integrity protection for TSF data and software and any user data stored by the TOE.
O.NON_REPUDIATION	The TOE will prevent a subscriber from avoiding accountability for sending a message by providing evidence that the subscriber sent the message; and control communications from unknown source.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. The TOE will protect data assets when they are being transmitted to and from the TOE, including through intervening untrusted components.
O.RECOVERY	The TOE will have the capability to store and recover to a previous state at the direction of the administrator (e.g., provide support for archival and recovery capabilities).
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE will provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data. The TOE will record in audit records: date and time of action and the entity responsible for the action.

O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only privileged users are able to log in and configure the TOE, and provide protections for logged-in users. The TOE will ensure that administrative responsibilities are separated across different roles in order to mitigate the impact of improper administrative activities or unauthorized administrative access.
O.TSF_SELF_TEST	The TOE will provide integrity protection to detect modifications to firmware, software, and archived data.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and from a trusted source.

The following table contains security objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	Environmental Security Objective Definition
OE.AUDIT_GENERATION	The Operational Environment provides a mechanism for the generation of portions of the audit data.
OE.CERT_REPOSITORY	The Operational Environment provides a certificate repository for storage of certificates (and optionally CRLs) issued by the TSF.
OE.CERT_REPOSITORY_SEARCH	The Operational Environment provides the ability to search a certificate repository for specific certificate fields in certificates issued by the TSF and return the certificate and an identifier for the certificate that can be used to search the audit trail for events related to that certificate.
OE.AUDIT_RETENTION	The Operational Environment provides mechanisms for retention of audit records for both normal and extended retention periods.
OE.AUDIT_REVIEW	The Operational Environment provides a mechanism for the review of specified audit data.
OE.AUDIT_STORAGE	The Operational Environment provides a mechanism for the storage of specified audit data.
OE.CRYPTOGRAPHY	The Operational Environment provides cryptographic services that can be invoked by the TSF in order to perform security functionality.
OE.KEY_ARCHIVAL	The Operational Environment provides the ability to use split knowledge procedures to enforce two-party control to export keys necessary to resume CA functionality if the TSF should fail.
OE.NO_GENERAL_PURPOSE	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.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.PUBLIC_KEY_PROTECTION	The Operational Environment provides protection for specified public keys associated with CA functions.
OE.SESSION_PROTECTION_LOCAL	The Operational Environment provides the ability to lock or terminate local administrative sessions.

OE.SESSION_PROTECTION_REMOTE	The Operational Environment provides the ability to lock or terminate remote administrative sessions.
OE.TOE_ADMINISTRATION	The Operational Environment provides specified management capabilities required for the overall operation of a Certificate Authority, and the ability to restrict access to a subset of the capabilities as specified in the ST.
OE.TRUSTED_ADMIN	The administrator of the TOE is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.
OE.TRUSTED_PLATFORM	The operating system on which the TOE has been installed is securely configured, regularly patched, and not subject to unauthorized access.

5 Requirements

As indicated above, requirements in the PP_CA_V2.1 are comprised of the "base" requirements and additional requirements that are optional, selection-based, or objective. The following table contains the "base" requirements that were validated as part of the CertAgent evaluation activities referenced above.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_ADP_EXT.1: Audit Dependencies	Information Security Corporation's CertAgent
	FAU_GCR_EXT.1: Generation of Certificate Repository	Information Security Corporation's CertAgent
	FAU_GEN.1 : Audit Data Generation	Information Security Corporation's CertAgent
	FAU_GEN.2: User Identity Association	Information Security Corporation's CertAgent
	FAU_STG.4: Prevention of Audit Data Loss	Information Security Corporation's CertAgent
FCO: Communications	FCO_NRO_EXT.2: Certificate-Based Proof of Origin	Information Security Corporation's CertAgent
FCS: Cryptographic Support	FCS_CDP_EXT.1: Cryptographic Dependencies	Information Security Corporation's CertAgent
	FCS_STG_EXT.1: Cryptographic Key Storage	Information Security Corporation's CertAgent
FDP: User Data Protection	FDP_CER_EXT.1: Certificate Profiles	Information Security Corporation's CertAgent
	FDP_CER_EXT.2: Certificate Request Matching	Information Security Corporation's CertAgent
	FDP_CER_EXT.3: Certificate Issuance Approval	Information Security Corporation's CertAgent
	FDP_CSI_EXT.1: Certificate Status Information	Information Security Corporation's CertAgent
	FDP_RIP.1: Subset Residual Information Protection	Information Security Corporation's CertAgent
FIA: Identification and Authentication	FIA_X509_EXT.1: Certificate Validation	Information Security Corporation's CertAgent

	FIA_X509_EXT.2: Certificate-Based Authentication	Information Security Corporation's CertAgent
	FIA_UAU_EXT.1: Authentication Mechanism	Information Security Corporation's CertAgent
	FIA_UIA_EXT.1: User Identification and Authentication	Information Security Corporation's CertAgent
FMT: Security Management	FMT_MOF.1(1): Management of Security Functions Behavior (Administrator Functions)	Information Security Corporation's CertAgent
	FMT_MOF.1(2): Management of Security Functions Behavior (CA/RA Functions)	Information Security Corporation's CertAgent
	FMT_MOF.1(3): Management of Security Functions Behavior (CA Operations Functions)	Information Security Corporation's CertAgent
	FMT_MOF.1(4): Management of Security Functions Behavior (Admin/Officer Functions)	Information Security Corporation's CertAgent
	FMT_MOF.1(5): Management of Security Functions Behavior (Auditor Functions)	Information Security Corporation's CertAgent
	FMT_MTD.1: Management of TSF Data	Information Security Corporation's CertAgent
	FMT_SMF.1: Specification of Management Functions	Information Security Corporation's CertAgent
	FMT_SMR.2: Restrictions on Security Roles	Information Security Corporation's CertAgent
FPT: Protection of the TSF	FPT_FLS.1: Failure with Preservation of Secure State	Information Security Corporation's CertAgent
	FPT_KST_EXT.1: No Plaintext Key Export	Information Security Corporation's CertAgent
	FPT_KST_EXT.2: TSF Key Protection	Information Security Corporation's CertAgent
	FPT_RCV.1: Manual Trusted Recovery	Information Security Corporation's CertAgent
	FPT_SKP_EXT.1: Protection of Keys	Information Security Corporation's CertAgent
	FPT_STM.1: Reliable Time Stamps	Information Security Corporation's CertAgent
	FPT_TUD_EXT.1: Trusted Update	Information Security Corporation's CertAgent
FTA: TOE Access	FTA_SSL.4: User-Initiated Termination	Information Security Corporation's CertAgent
	FTA_TAB.1: Default TOE Access Banners	Information Security Corporation's CertAgent
FTP: Trusted Path/Channels	FTP_TRP.1: Trusted Path	Information Security Corporation's CertAgent

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_COP.1(5): Cryptographic Operation (Password-Based Key Derivation Function)	Information Security Corporation's CertAgent
FDP: User Data Protection	FDP_CER_EXT.4: Non-X.509v3 Certificate Generation	PP Evaluation
	FDP_SDP_EXT.1: User Sensitive Data Protection	PP Evaluation
	FDP_STG_EXT.1: Public Key Protection	Information Security Corporation's CertAgent
FPT: Protection of the TSF	FPT_NPE_EXT.1: NPE Constraints	PP Evaluation
	FPT_SKY_EXT.1: Split Knowledge Procedures	PP Evaluation
	FPT_TST_EXT.1: TOE Integrity Test	PP Evaluation
	FPT_TST_EXT.2: Integrity Test	Information Security Corporation's CertAgent
FTA: TOE Access	FTA_SSL.3: TSF-Initiated Termination	Information Security Corporation's CertAgent
	FTA_SSL_EXT.1: TSF-Initiated Session Locking	PP Evaluation

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_SAR.1: Audit Review	Information Security Corporation's CertAgent
	FAU_SAR.3: Selectable Audit Review	Information Security Corporation's CertAgent
	FAU_SCR_EXT.1: Certificate Repository Review	Information Security Corporation's CertAgent
	FAU_SEL.1: Selective Audit	Information Security Corporation's CertAgent
	FAU_STG.1(1): Protected Audit Trail Storage	PP Evaluation
	FAU_STG.1(2): Protected Audit Trail Storage (Archive Data)	PP Evaluation
	FAU_STG_EXT.1: External Audit Trail Storage	Information Security Corporation's CertAgent
	FAU_STG_EXT.2: Audit Data Retention	PP Evaluation
FCS: Cryptographic Support	FCS_CKM_EXT.1(1): Symmetric Key Generation for DEKs	Information Security Corporation's CertAgent
	FCS_CKM.1: Cryptographic Key Generation	Information Security Corporation's CertAgent

	FCS_CKM.2: Cryptographic Key Establishment	Information Security Corporation's CertAgent
	FCS_CKM_EXT.1(2): Key Generation Key Encryption Keys	Information Security Corporation's CertAgent
	FCS_CKM_EXT.1(3): Key Generation for Key Encryption Keys (TOE Key Archival)	PP Evaluation
	FCS_CKM_EXT.1(4): Generation of Key Shares	PP Evaluation
	FCS_CKM_EXT.4: Cryptographic Key Destruction	Information Security Corporation's CertAgent
	FCS_CKM_EXT.5: Public Key Integrity	Information Security Corporation's CertAgent
	FCS_CKM_EXT.6: TOE Key Archival	PP Evaluation
	FCS_CKM_EXT.7: Key Generation for KEKs	PP Evaluation
	FCS_CKM_EXT.8: Key Hierarchy Entropy	Information Security Corporation's CertAgent
	FCS_COP.1(1): Cryptographic Operation (AES Encryption/Decryption)	Information Security Corporation's CertAgent
	FCS_COP.1(2): Cryptographic Operation (Cryptographic Signature)	Information Security Corporation's CertAgent
	FCS_COP.1(3): Cryptographic Operation (Cryptographic Hashing)	Information Security Corporation's CertAgent
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)	Information Security Corporation's CertAgent
	FCS_HTTPS_EXT.1: HTTPS Protocol	Information Security Corporation's CertAgent
	FCS_IPSEC_EXT.1: IPsec Protocol	PP Evaluation
	FCS_TLSC_EXT.1: TLS Client Protocol	PP Evaluation
	FCS_TLSC_EXT.2 TLS Client Protocol with Mutual Authentication[i]	PP Evaluation
	FCS_TLSS_EXT.1; TLS Server Protocol	Information Security Corporation's CertAgent
	FCS_TLSS_EXT.2: TLS Client Protocol with Mutual Authentication[ii]	Information Security Corporation's CertAgent
	FCS_RBG_EXT.1: Cryptographic Random Bit Generation	Information Security Corporation's CertAgent
FCO: Communications	FCO_NRR_EXT.2: Certificate-Based Proof of Receipt	PP Evaluation
FDP: User Data Protection	FDP_CRL_EXT.1: Certificate Revocation List Validation	Information Security Corporation's CertAgent
	FDP_ITT.1: Basic Internal Transfer Protection	PP Evaluation
	FDP_OCSPG_EXT.1: OCSP Basic Response Generation	Information Security Corporation's CertAgent
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling	PP Evaluation
	FIA_CMCS_EXT.1: Certificate Management over CMS (CMC) Server	PP Evaluation
	FIA_CMCC_EXT.1: Certificate Management over CMS (CMC) Client	PP Evaluation

	FIA_ESTS_EXT.1: Enrollment over Secure Transport (EST) Server	Information Security Corporation's CertAgent
	FIA_ESTC_EXT.1: Enrollment over Secure Transport (EST) Client	PP Evaluation
	FIA_PMG_EXT.1: Password Management	PP Evaluation
	FIA_PSK_EXT.1: Pre-Shared Key Composition	PP Evaluation
	FIA_UAU.7: Protected Authentication Feedback	PP Evaluation
	FIA_X509_EXT.3: X509 Certificate Request	Information Security Corporation's CertAgent
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Privileged User Passwords	PP Evaluation
	FPT_ITT.1 Basic Internal TSF Data Transfer Protection	PP Evaluation
	FPT_SKY_EXT.2: Key Share Access	PP Evaluation
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	Information Security Corporation's CertAgent

The following table contains the "**Objective**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation".

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_KSH_EXT.1: Key Sharing	PP Evaluation
FIA: Identification and Authentication	FIA_ESTC_EXT.2: EST Client use of TLS-unique value	PP Evaluation
	FIA_ESTS_EXT.2: Enrollment over Secure Transport (EST) Server	PP Evaluation
	FIA_ENR_EXT.1.1: Certificate Enrollment	Information Security Corporation's CertAgent

6 Assurance Requirements

The following are the assurance requirements contained in the PP_CA_V2.1.

Table 10: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Information Security Corporation's CertAgent
	ASE_ECD.1: Extended Components Definition	Information Security Corporation's CertAgent
	ASE_INT.1: ST Introduction	Information Security Corporation's CertAgent

	ASE_OBJ.1: Security Objectives for the Operational Environment	Information Security Corporation's CertAgent
	ASE_REQ.1: Stated Security Requirements	Information Security Corporation's CertAgent
	ASE_SPD.1: Security Problem Definition	Information Security Corporation's CertAgent
	ASE_TSS.1: TOE Summary Specification	Information Security Corporation's CertAgent
ADV: Development	ADV_FSP.1 Basic Functional Specification	Information Security Corporation's CertAgent
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Information Security Corporation's CertAgent
	AGD_PRE.1: Preparative Procedures	Information Security Corporation's CertAgent
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Information Security Corporation's CertAgent
	ALC_CMS.1: TOE CM Coverage	Information Security Corporation's CertAgent
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Information Security Corporation's CertAgent
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Information Security Corporation's CertAgent

7 Results of the Evaluation

Note that for APE elements and work units that are identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 11: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Information Security Corporation's CertAgent; PP evaluation
APE_ECD.1	Pass	Information Security Corporation's CertAgent; PP evaluation
APE_INT.1	Pass	Information Security Corporation's CertAgent; PP evaluation
APE_OBJ.1	Pass	Information Security Corporation's CertAgent; PP evaluation
APE_REQ.1	Pass	Information Security Corporation's CertAgent; PP evaluation
APE_SPD.1	Pass	Information Security Corporation's CertAgent; PP evaluation

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and

approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the PP_CA_V2.1 Evaluation Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this 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, dated: April 2017.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: 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, dated: April 2017.

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

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Protection Profile for Certification Authorities, Version 2.1, 01 December 2017.

[7] CertAgent Security Target for Common Criteria Evaluation, Software Version 7.0, Document Version 4.1.1, 11 July 2018.

[8] Assurance Activity Report for CertAgent version 7.0, Document Version 1.5a, 17 July 2018.

[i] This SFR is not part of the original published PP_CA_V2.1 but was amended by NIAP TD0294 (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=300)

[ii] This SFR is not part of the original published PP_CA_V2.1 but was amended by NIAP TD0294 (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=300)