# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme

# Validation Report

# for the

# INTEGRITY Enterprise OS – Archon Edition

| | |
|---|---|
| **Report Number:** | **CCEVS-VR-11258-2022** |
| **Dated:** | **05/03/2022** |
| **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

## Validation Team

Jim Donndelinger

Swapna Katikaneni

Dave Thompson

*The Aerospace Corporation*

## Common Criteria Testing Laboratory

Anthony Busciglio

Lucas Shaefer

*Acumen Security, LLC*

# Table of Contents

# 1 Executive Summary

This Validation Report (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 for 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 tested and evaluated and any restrictions on the evaluated configuration. 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 the INTEGRITY Enterprise OS – Archon Edition Target of Evaluation (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 applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in May 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the Protection Profile for General Purpose Operating Systems Version 4.2.1, dated 2019-04-22 [OSPP].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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), as interpreted by the Assurance Activities contained in the Protection Profile for General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP]. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation 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 Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against the Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Compliance 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.
- The Protection Profile(s) 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** | INTEGRITY Enterprise OS – Archon Edition Version 1.0 |
| **Protection Profile** | Protection Profile for General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP] |
| **Security Target** | INTEGRITY Enterprise OS – Archon Edition Security Target version 1.2 dated April 26,2022 |
| **Evaluation Technical Report** | Evaluation Technical Report for INTEGRITY Enterprise OS - Archon Edition, 1.0 version 1.0 |
| **CC Version** | Version 3.1, Revision 5 |
| **Conformance Result** | CC Part 2 Extended and CC Part 3 Extended |
| **Sponsor** | Archon Secure LLC |
| **Developer** | Archon Secure LLC |
| **Common Criteria Testing Lab (CCTL)** | Acumen Security<br>Rockville, MD |
| **CCEVS Validators** | Jim Donndelinger, Swapna Katikaneni, Dave Thompson<br>The Aerospace Corporation |

# 3 Architectural Information

The TOE is the INTEGRITY Enterprise OS – Archon Edition, which provides a secure computing environment for mobile platforms.  The TOE provides end users with the ability to install their own custom user software in a high security sandbox, while maintaining a secure operating system enclave logically isolated from the end user’s application.

# 4 Security Policy

The TOE implements the following security functional requirements from [OSPP] as listed below:

## 4.1 Audit Data Generation (FAU)

The TOE audits the following events and details:

- Audit all administrative functions.
- Audit all security-relevant functions of the OS.
- Audit the causing user, calling process, and specific error messages for any logged events.

## 4.2 Cryptographic Support (FCS)

The TOE includes the INTEGRITY Crypto Library v1.0 (ICL). Functions implemented with ICL are in service of all cryptographic functionality required by the SFRs. The TOE supports the following cryptographic functions:

| SFR | Cryptographic Algorithm | Operating Env. | Modes & Key Sizes | CAVP |
|---|---|---|---|---|
| FCS_CKM.1 | *ECC KeyGen in accordance with FIPS 186-4 Appendix B.4* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | NIST Curves P-256, P-384, P-521 | C1871 |
| FCS_CKM.2 | *Elliptic Curve key establishment in accordance with NIST SP 800-56A* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | NIST Curves P-384 | C1871 |
| FCS_COP.1(1) | *AES-XTS in accordance with NIST SP 800-38E* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | 256-bit | C1871 |
| | *AES-GCM in accordance with NIST SP 800-38D* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | 256-bit | C1871 |
| FCS_COP.1(2) | *SHA-1, SHA-256, SHA-384, SHA-512 in accordance with FIPS Pub 180-4* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | 160 bits for SHA-1, 256 bits for SHA-256; 384 bits for SHA-384; 512 bits for SHA-512 | C1871 |
| FCS_COP.1(3) | *ECDSA SigGen and SigVer in accordance with FIPS Pub 186-4 Section 5* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | NIST curve P-384 | C1871 |
| | *RSA SigGen and SigVer in accordance with FIPS Pub 186-4* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | 2048-bit | C1871 |
| FCS_COP.1(4) | *SHA-1, SHA-256, SHA-384, SHA-512 in accordance with FIPS Pub 198-1 and FIPS Pub 180-4* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | For SHA-256, a 256-bit key size and message size.<br>For SHA-384, a 384-bit key size and message size.<br>For SHA-512, a 512-bit key size and message size. | C1871 |

| SFR | Cryptographic Algorithm | Operating Env. | Modes & Key Sizes | CAVP |
|---|---|---|---|---|
| FCS_RBG_EXT.1 | *HMAC_DRBG in accordance with NIST SP 800-90A* | SWIC Operating System 1.0 on INTEGRITY-IoT-2020.24 RTOS Microkernel | Random number generation for all cryptography | C1871 |

## 4.3 User Data Protection (FDP)

The TOE protects all user data on disk via always-on encryption. All data on the disk, including the OS files and all user data, are automatically encrypted. This includes all Protection Profile-defined Sensitive Data, including:

- User application private keys, secrets, and key material.
- Certificates and keys used for trusted path establishment, trusted channel establishment, and trusted update verification.

## 4.4 Identification and Authentication (FIA)

The TOE implements user identification and authentication, including authentication failure limiting, at all administrative interfaces. No more than three consecutive unsuccessful authentication attempts on any given power cycle. The TOE requires that the administrator successfully authenticate prior to performing any management or configuration functions.

The TOE supports the use of X.509v3 certificates, including revocation and validity checking. The administrator may choose which certificate is used for any given trusted path or trusted channel.

## 4.5 Security Management (FMT)

The TOE permits authorized and authenticated administrators to perform the following management functions:

- Set the inactivity timeout.
- Configure trusted paths and channels.
- Configure the networking parameters.
- Configure automatic updates.
- Management of user accounts.

## 4.6 Protection of the TSF (FPT)

The TOE implements protection of the kernel, audit logs and functions, and credential repositories. The TOE implements Address Space Layout Randomization and Stack-Based Buffer Overflow protection. The TOE performs self-tests of the cryptographic functions prior to operation and implements security checking prior to installing updates.

## 4.7 Trusted Paths and Channels (FTP)

The TOE provides a TLS trusted communication path to both administrators and trusted IT entities that protects the channel data from modification or compromise.

# 5 Assumptions, Threats & Clarification of Scope

## 5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's 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.

| ID | Assumption |
|---|---|
| A.PLATFORM | The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP. |
| A.PROPER_USER | The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope. |
| A.PROPER_ADMIN | The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy. |

## 5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

| ID | Threat |
|---|---|
| T.NETWORK_ATTACK | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications. |
| T.NETWORK_EAVESDROP | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS. |
| T.LOCAL_ATTACK | An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system. |

| | |
|---|---|
| T.LIMITED_PHYSICAL_ACCESS | An attacker may attempt to access data on the OS while having a limited amount of time with the physical device. |

### 5.3 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 level of assurance for this evaluation is defined within the Protection Profile for General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP].
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- The evaluated configuration of the TOE is the INTEGRITY Enterprise OS – Archon Edition Version 1.0 software product and not any earlier or later versions released or in process.

# 6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- INTEGRITY Enterprise OS – Archon Edition Security Target version 1.2
- INTEGRITY Enterprise OS – Archon Edition Common Criteria Administrative Guidance version 1.2

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

# 7 TOE Evaluated Configuration

## 7.1 Evaluated Configuration

The TOE is the INTEGRITY Enterprise OS – Archon Edition, which provides secure computing on the Archon ZV secure mobility platform. This includes the bootloader and all code that executes from device power on until the full OS is loaded, and runs only on the secure mobile platforms below:

| Platform Name | CPU | HDD | RAM |
|---|---|---|---|
| Archon ZV 5400 | Intel Core i5-8365U (Whiskey Lake 64-bit microarchitecture) | 250 GB | 8 GB or 16GB |

Furthermore, the TOE requires the operational environment to provide the following to support its security functions:

- For administration of the TOE, at least one authorized administration server.
- For TOE updates, at least one authorized update server.
- For handling of TOE-generated audit records, at least one authorized audit server.

## 7.2 Excluded Functionality

The following interfaces are not included as part of the evaluated configuration:

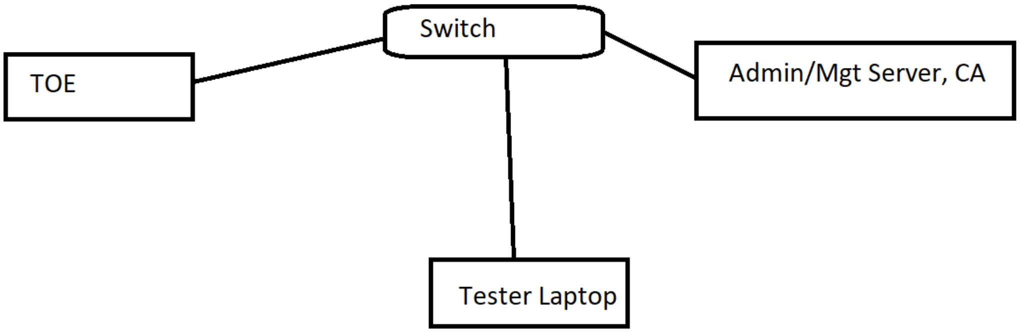
| Functions | Exclusion discussion |
|---|---|
| None | All TOE functions are evaluated as part of the Common Criteria Evaluation. |

# 8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for INTEGRITY Enterprise OS – Archon Edition, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

## 8.1 Test Configuration

Testing was carried at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850 by the evaluator. Testing occurred from February 2021 through February 2022. Testing was performed within Acumen's Common Criteria lab in a controlled, isolated environment using the test configuration depicted below and completed by the Acumen Security Evaluation Team following the CCTL's NVLAP-accredited test procedure.



| Name | OS | Version | Function & Location | Protocols | Tools (version) |
|---|---|---|---|---|---|
| Archon ZV 5400 | INTEGRITY Enterprise OS | Archon Edition 1.0 | TOE | TLS<br>ICMP | • Anyconnect VPN 4.7<br>• Aruba VPN 3.4 |
| Administration/ Management Server | Ubuntu 20 | Archon Edition 1.0 | Third-party VPN Testing | ICMP<br>ISAKMP<br>ESP | • INTEGRTY Administration Server (Archon Edition 1.0)<br>• INTEGRITY Management Server (Archon Edition 1.0)<br>• Anyconnect VPN (4.7)<br>• Aruba VPN (3.4)<br>• Wireshark (3.0) |
| Administration/ Management Server | Ubuntu 20 | Archon Edition 1.0 | Third-party VPN Testing | ICMP | • INTEGRTY Administration Server (Archon Edition 1.0)<br>• INTEGRITY Management Server (Archon Edition 1.0)<br>• Anyconnect VPN (4.7)<br>• Aruba VPN (3.4) |

| Name | OS | Version | Function & Location | Protocols | Tools (version) |
|---|---|---|---|---|---|
| | | | | | - Wireshark (3.0) |
| Network Switch | IOS XE | 15.2 | Lab Switch | N/A | N/A |
| Administration/ Management Server | Ubuntu 20 | Archon Edition 1.0 | Remote administration<br>TLS/X509 Testing<br>Certificate Authority | TLS | - INTEGRTY Administration Server (Archon Edition 1.0)<br>- INTEGRITY Management Server (Archon Edition 1.0)<br>- OpenSSL (1.1.1)<br>- Acumen_TLSC (8-23-21)<br>- Wireshark (3.0) |
| Tester Laptop | Windows 10 | 10 | Test Interface | TLS | N/A |

## 8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

## 8.3 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

# 9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

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 rev 5 and CEM version 3.1 rev 5. The evaluation determined the INTEGRITY Enterprise OS – Archon Edition to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

## 9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the INTEGRITY Enterprise OS – Archon Edition that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP].

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP] related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

## 9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP] related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

## 9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP] and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP], and that the conclusion reached by the evaluation team was justified.

## 9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP], and that the conclusion reached by the evaluation team was justified.

## 9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities 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 performed the Assurance Activities in the General Purpose Operating Systems, version 4.2.1, dated 2019-04-22 [OSPP], and correctly verified that the product meets the claims in the ST.

# 10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the INTEGRITY Enterprise OS – Archon Edition Common Criteria Administrative Guidance version 1.2 document. No versions of the TOE and software, either earlier or later were evaluated.

# 11 Annexes

Not applicable.

# 12 Security Target

INTEGRITY Enterprise OS – Archon Edition Security Target version 1.2 dated April 26,2022

# 13 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 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.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **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.

# 14 Bibliography

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

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.