National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Nubo Client Version 3.2

Report Number: CCEVS-VR-VID11380-2023

Dated: December 20, 2023

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

Lauren Brandt
Lisa Mitchell
Linda Morrison
Clare Parran

The MITRE Corporation

Common Criteria Testing Laboratory

George Kumi
Shaunak Shah
Joan Marshall
Shaina Rae

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 Nubo Client Version 3.2 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 December 2023. 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 Extended and meets the assurance requirements of the *Protection Profile for Application Software*, version 1.4, 2021-10-07 [PP_APP] and *Functional Package for Transport Layer Security (TLS)*, version 1.1, 2019-03-01 [PKG_TLS].

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 (PP). This VR 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 ETR 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 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 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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 Compliant 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	Nubo Client Version 3.2
Security Target	*Nubo Client Version 3.2 Security Target*, version 1.18, 15 December 2023
Sponsor & Developer	Nubo Software, LTD
Protection Profile	• *Protection Profile for Application Software*, version 1.4, 2021-10-07 [PP_APP] • *Functional Package for Transport Layer Security (TLS)*, version 1.1, 2019-03-01 [PKG_TLS]
CC Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
Validation Personnel	Lauren Brandt, Lisa Mitchell, Linda Morrison, Clare Parran

3 Architectural Information

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

The Target of Evaluation (TOE) is the Nubo Client Version 3.2. It is a thin client application installed and executed on an Android mobile device. The TOE establishes communications to a Virtual Mobile Infrastructure (VMI) platform (using a remote display protocol) and remotely displays the virtual apps that are running within the VMI platform. No output is displayed from other applications. The TOE only connects the mobile device to the virtual servers and is not responsible for the execution of the virtual apps.

With VMI, virtual applications execute on a user's behalf on VMI servers. No executable code associated with the virtual applications is downloaded to the user's device. Instead, the TOE displays the output from the virtual applications, and forwards input from the user to the virtual applications.

The TOE controls all communication between itself and the VMI environment. The TOE is only to be used with the Nubo Management Server and the Nubo Gateway. This ensures that all communication occurs over a secure connection within a secure remote application infrastructure. All network connections are initiated by the TOE. Connection requests by a VMI server are not accepted.

Direct connection is established between the TOE and the Nubo Management Server. The Nubo Management Server processes user activation and login and communicates with the TOE and the Nubo Gateway. The Nubo Gateway implements the connection for executing the virtual applications. The traffic for the virtual applications (that are transmitted from the VMI platform to the Nubo Gateway) is sent over a single trusted channel between the Management Server and the TOE.

The user installs the TOE from the Google Play Store. The app store contains a generic version of the Android app which does not contain any user credentials or details. Initially, TOE user credentials are sent to the Management Server, the Management Server registers the TOE user, the user activates the TOE, and connects to the Nubo Management Server. Once registered, the user is required to authenticate itself to the Management server on successive sessions with the VMI environment.

3.1 TOE Description

The TOE is the thin client executing on mobile devices. It implements a user interface to virtual mobile applications executing on Nubo Software's VMI servers. The TOE runs on the evaluated Samsung Galaxy S10 device with Android 12 operating system.

The TOE was tested on the following mobile device:

Device Name	Chipset Vendor	SoC	Base Model Number	32 bit/64 bit
Galaxy S10	Qualcomm	Snapdragon 855	SM-G973	64 bit

3.1.1 Software Requirements

Operating system: Android 12.0, Linux kernel 4.14.

3.1.2 Hardware Requirements

A Samsung Galaxy S10 mobile device.

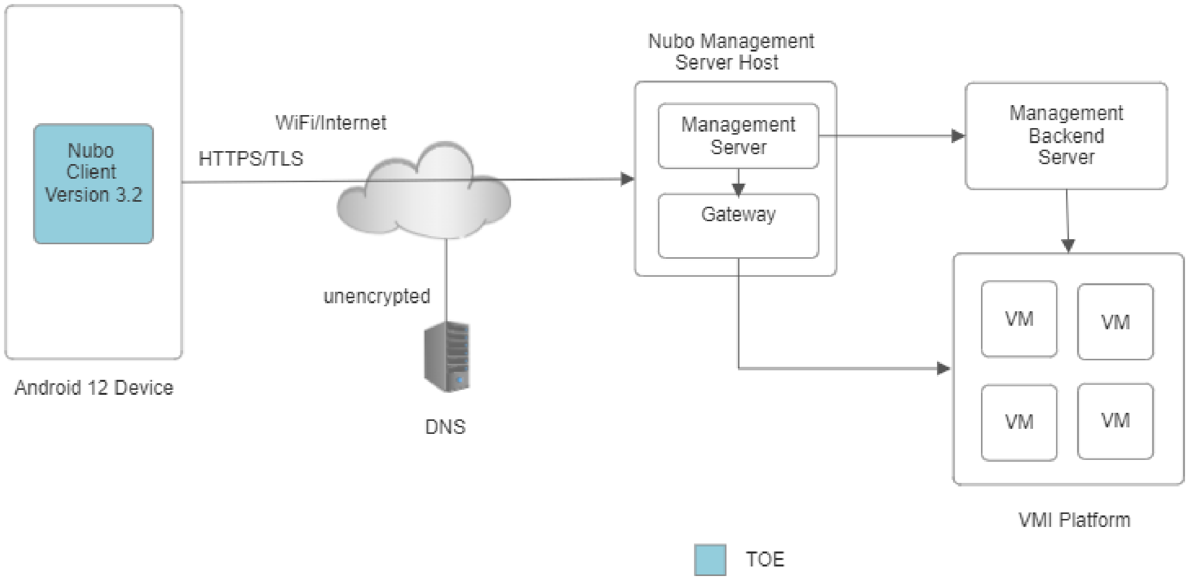
3.2 Physical Boundary

The physical boundary of the TOE is:

1) the thin client Android application (TOE): Nubo Client Version 3.2 installed and running on a supported platform.

3.3 TOE Operational Environment

The TOE's operational environment is illustrated below. The TOE is the client App and is as defined in this ST and highlighted in the figure. Other components constitute the Nubo thin client infrastructure required for the full operation of the TOE.



The following external components are required by the TOE:

- Android 12 OS platform required to host the TOE (refer to section 3.1 for the platform options).
- Platform connection to the Internet – either using WiFi or Cellular wireless service.
- DNS Server – access to a Domain Name System Server to resolve FQDN to IP addresses. Access is automatic if connected to a WiFi or Cellular wireless service.

- Nubo Management Server Host – a frontend server host running Nubo Management Server and Nubo Gateway. TOE users are instructed in the ancillary guidance document that the URL of this host is https://cc.nubo.co.
- Nubo Management Server – a frontend software server running on the Nubo Server Management Host that processes TOE user activation and login and communicates with the Nubo Gateway, the Management Backend Server, and the TOE.
- Nubo Gateway – a frontend application running on the Nubo Management Server Host that implements the connection for executing the virtual applications and communicates with the Nubo Management Server.
- Management Backend Server – a backend server that supports databases and other supporting services for the Nubo Management Server Host and the VMI Platform.
- VMI platform – A host supporting multiple virtual machines. At least one VM is required.

The Nubo Server is configured with information about the Nubo Gateway, Management Backend Server, VMI platforms, and VMs. Therefore, the configuration of the backend environment is not required by the TOE.

4 Security Policy

The TOE implements the security functions and security mechanisms identified in the following sections.

4.1 Cryptographic Support

The TOE implements cryptographic functions for DRBG, key establishment, TLS and HTTPS protocols, and X.509 certificate validation. The TOE implements TLS using BoringSSL Library which in turn implements cryptographic functions using the BoringCrypto Library.

4.2 User Data Protection

The TOE stores sensitive user data (such as the user’s full name and email address) encrypted in local files. These files are private to the TOE. The TOE also stores unencrypted cache files of graphical resources that are fetched from the server, which are pre-defined as non-sensitive data. The TOE can access physical resources on the mobile device but does not store locally any data fetched from a physical resource.

4.3 Identification and Authentication

The identification of a user is comprised of the email address of the user and a unique client activation code, which identifies the specific TOE installation on a specific device. Authentication of the user of the TOE to the Nubo Management Server is one factor.

4.4 Security Management

The TOE does not have default credentials. The user selects the credentials when registering to the Management Server. The TOE uses the platform mechanism for storing configuration settings.

When the TOE is installed for the first time, it is not recognized by the remote system and must be activated prior to becoming operational. The user sends an activation request to which the Management Server responds either by a Client Activation Key or by a rejection of the activation. If activation is successful, the TOE saves the Client Activation Key in the Android keystore.

Once installed, the TOE may be upgraded and patches may be obtained from the Google Play Store if an appropriate upgrade is available.

4.5 Privacy

Personal Identifiable Information (PII) collected during the activation is transmitted to the Management Server over a trusted channel. The PII is a password created by the user. User consent is required before transmitting the information to the server.

4.6 Protection of the TSF

The Android platform provides protection of the TSF data. The platform protection mechanisms include checks that the TOE is properly signed and protection of the TOE and TOE Data from access by other apps. Secure delivery of the TOE and updates is accomplished though the delivery of the TOE and updates from the Google Play Store.

4.7 Trusted Channels

The TOE establishes a TLS 1.2 connection for all communications with the Management Server. The channel is used for identification, configuration, authentication, receiving remote display data from the virtual apps, and sending user input data to the servers and to the virtual apps.

5 Assumptions & 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:

- The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in PP_APP_V1.4 and PKG_TLS_V1.1 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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 Application Software*, version 1.4, 2021-10-07 [PP_APP] and *Functional Package for Transport Layer Security (TLS)*, version 1.1, 2019-03-01 [PKG_TLS].
- 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 evaluation of security functionality of the product was limited to the functionality specified in *Nubo Client Version 3.2 Security Target*, Version 1.18, 15 December 2023. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- 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 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:

- *Nubo Client Version 3.2 Guidance Document*, 15 December 2023

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 developer and the evaluation team. It is derived from information contained in the proprietary *Test Plan for Nubo Client Version 3.2*, version 1.4, 15 December 2023. The *Assurance Activity Report for Nubo Client Version 3.2,* Version 1.10, 18 December 2023 provides a non-proprietary overview of testing and the prescribed assurance activities.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

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 the following specifications:

- *Protection Profile for Application Software*, version 1.4, 2021-10-07 [PP_APP]
- *Functional Package for Transport Layer Security (TLS)*, version 1.1, 2019-03-01 [PKG_TLS]

The evaluation team devised a test plan based on the test activities specified in the PP and FP. 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 test report listed above.

All testing was carried out at the Acumen Security offices located at 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from October 2022 to December 2023. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE was evaluated on the following platform installed with Android 12.

Device Name	Chipset Vendor	SoC	Base Model Number
Galaxy S10	Qualcomm	Snapdragon 855	SM-G973

8.2 Excluded Functionality

- Fingerprint authentication functionality has been excluded from the evaluation.
- The evaluated configuration only supports the default Nubo Management Server Host (https://cc.nubo.co).

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 ETR. The reader of this document can assume that all 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 TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team performed each TSS evaluation 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 PP, and security function descriptions that satisfy the requirements.

The validation team 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 performed each ADV evaluation 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 PP 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.

The validation team 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 performed each guidance evaluation 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.

The validation team 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 performed each ALC evaluation 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 PP. 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.

The validation team 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 performed each test activity and applied each ATE_IND.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.

The validation team 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.

9.6 Vulnerability Assessment Activity

The evaluation team performed each AVA evaluation 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.

The evaluation team examined the following sources of publicly available information to identify potential vulnerabilities in the TOE:

- https://nvd.nist.gov/view/vuln.search
- http://cve.mitre.org/cve
- https://www.cvedetails.com/vulnerability-search.php
- https://www.kb.cert.org/vuls/search/
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search

- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com
- https://www.rapid7.com/db/vulnerabilities

The evaluation team performed searches on 10/20/2023 and 12/07/2023 using the following search terms:

- Nubo Client
- The 3rd party libraries listed in the ST
- The APIs listed in the TSS within the ST

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.

The validation team 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.

9.7 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 PP. 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 followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable.

12 Security Target

- *Nubo Client Version 3.2 Security Target*, Version 1.18, 15 December 2023

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.
5. *Protection Profile for Application Software*, Version 1.4, 2021-10-07.
6. *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 2019-03-01.
7. *Nubo Client Version 3.2 Security Target*, Version 8, 15 December 2023.
8. *Nubo Client Version 3.2 Guidance Document*, 15 December 2023.
9. *Assurance Activity Report for Nubo Client Version 3.2*, Version 1.10, 18 December 2023 (AAR).
10. *Evaluation Technical Report (ETR) for Nubo Client Version 3.2*, 3, 15 December 2023.
11. *Vulnerability Assessment for Nubo Client Version 3.2*, Version 1.3, December 15, 2023.
12. *Test Plan for Nubo Client Version 3.2*, Version 1.4, 15 December 2023.