National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Perspecta Labs SecureIO v2.0.4

Report Number:	**CCEVS-VR-VID11170-2021**
Dated:	**July 12, 2021**
Version:	**1.0**

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Jenn Dotson

The MITRE Corporation

Farid Ahmed
Joyce Baidoo

Johns Hopkins Applied Physics Lab

Common Criteria Testing Laboratory

Sai Sandeep Yanamandra
Harshada Khandagale
Shaina Rae
Shaunak Shah

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Perspecta Labs SecureIO v2.0.4 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 Security Target (ST).

The evaluation was completed by Acumen Security in July 2021. 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 Application Software*, Version 1.3, dated 01 March 2019 [SWAPP].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). 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 (CCEVS) 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.

The technical information included in this report was obtained from the *Perspecta Labs SecureIO v2.0.4 Security Target*, Version 0.8, June 30, 2021, and analysis performed by the Validation team.

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) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology 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 TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile (PP) 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	Perspecta Labs SecureIO v2.0.4
Protection Profile	*Protection Profile for Application Software*, Version 1.3, dated, 01 March 2019 [SWAPP].
Security Target	*Perspecta Labs SecureIO v2.0.4 Security Target*, Version 0.8, June 30, 2021
Evaluation Technical Report	*Evaluation Technical Report for Perspecta Labs SecureIO v 2.0.4*, Version 0.2, June 2021
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Perspecta Labs
Developer	Perspecta Labs
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Paul Bicknell, Jenn Dotson, Farid Ahmed, Joyce Baidoo

3 Architectural Information

The SecureIO application provides a secure communication channel for Android applications by transmitting and receiving network traffic over a secure TLS channel. The traffic will be protected in transit using TLS between the Android device and a TLS server. Figure 1 below provides an overview and indicates the TOE boundary with a red-dotted line.

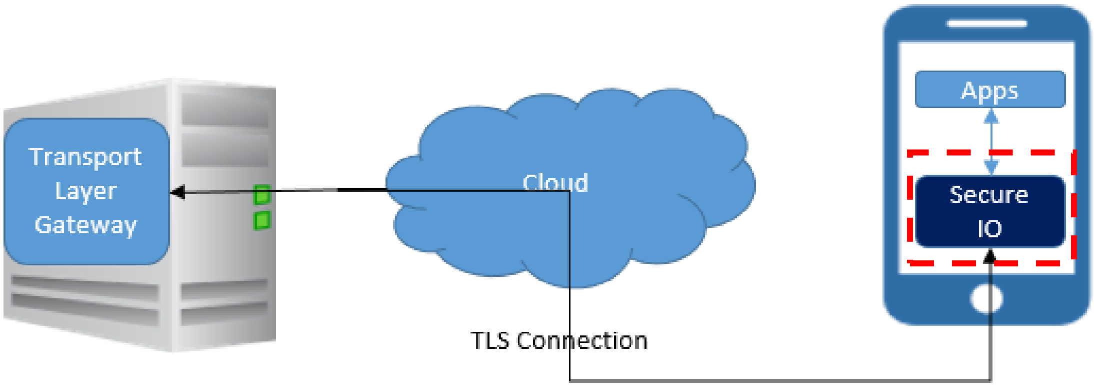

Figure 1 SecureIO Overview

The functionality of the SecureIO service is limited to (i) establishing and shutting down a TLS connection to the Transport Layer Gateway (TLG); (ii) sending and receiving messages to and from the TLG on behalf of Android apps via the TLS connection.

The TOE runs on Android versions 8.0, 9.0, and 10.0. All sub-versions of 8.0 (e.g. 8.1.0), 9.0 and 10.0 are supported.

4 Security Policy

The TOE provides the security functionality required by the Protection Profile for Application Software Version 1.3 [SWAPP].

4.1 Cryptographic Support

The TOE relies on underlying cryptographic functionality provided by the platform for all of its cryptographic operations.

4.2 User Data Protection

The TOE is a TLS proxy that encrypts data sent by other applications on its host platform.

4.3 Security Management

The TOE does not come with any default credentials. It identifies itself to the TLS gateway that it connects to using a certificate and private key. These are provisioned onto the TOE by an administrator or end user.

4.4 Privacy

The TOE itself does not contain or transmit any PII. It functions as a TLS proxy over which other applications on the platform may transmit whatever data they wish.

4.5 Protection of the TSF

The TOE employs several mechanisms to ensure that it is secure on the host platform. Only documented platform APIs are used by the TOE. The TOE never allocates memory with both write and execute permission. Evaluated platform functionality is used to verify the TOE version and perform updates, and no third-party libraries are used.

4.6 Trusted Path/Channels

TLS is used to protect all data transmitted to and from the TOE.

4.7 Identification and Authentication

Certificate validation and certificate authentication are performed by the TOE as part of TLS, in accordance with RFC 5280.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions & Threats

The Security Problem Definition, including the assumptions and threats, may be found in the following document:

- *Protection Profile for Application Software*, Version 1.3, dated, 01 March 2019 [SWAPP].

That information has not been reproduced here and the SWAPP should be consulted if there is interest in that material.

5.2 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *Protection Profile for Application Software*, Version 1.3, dated 01 March 2019 [SWAPP].
- This evaluation covers the specific versions of software as identified in this document, and not earlier or later versions released or in process.
- Consistent with the expectations of the PP, 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 scope of this evaluation was limited to the functionality and assurances covered in the SWAPP and applicable Technical Decisions 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.

6 Documentation

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

- [ST] *Perspecta Labs SecureIO v2.0.4 Security Target*, Version 0.8, June 30, 2021
- [AGD] *Perspecta Labs SecureIO User Manual*, *Version 2.0.4*, Issue 6, June 2021

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a software application that resides entirely on its Android-based mobile platform. The TOE runs on Android versions 8.0, 9.0, and 10.0. All sub-versions of 8.0 (e.g. 8.1.0), 9.0 and 10.0 are supported. The TOE was tested and evaluated on Samsung S8 running Android 8.0, Samsung S9 running Android 9.0, and Samsung S10 running Android 10.0.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in the *Assurance Activity Report for Perspecta Labs SecureIO v2.0.4*, Version 0.2, June 30, 2021 [AAR]. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the SWAPP. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here. Testing took place between May 2020 and June 2021 at the Acumen Security offices.

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 Reports (DTR) and the 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 Perspecta Labs SecureIO v2.0.4 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the SWAPP.

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 Perspecta Labs SecureIO v2.0.4 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 SWAPP.

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 applied each 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 SWAPP related to the examination of the information contained in the TOE Summary Specification.

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 applied each 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 SWAPP related to the examination of the information contained in the operational guidance documents.

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 applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

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 applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Assurance Activities in the SWAPP and recorded the results in a Test Reports, summarized in the ETR and AAR.

The Validation team 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 SWAPP, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Vulnerability Assessment Report prepared by the Evaluation team. The Evaluation team performed a public search for vulnerabilities and did not discover any open vulnerabilities.

The Evaluation team searched:

- 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
- https://www.peratonlabs.com/secureio.html

The search was performed on June 29, 2021, with the following search terms:

- SecureIO v2.0.4, SecureIO
- Perspecta Labs
- Samsung Galaxy S8
- Samsung Galaxy S9
- Samsung Galaxy S10
- Samsung Android 8
- Samsung Android 9
- Samsung Android 10
- Samsung Knox – Extra security layer/API on devices on which TOE operates.
- Boring SSL – Crypto Library Accessed via the AndroidAPI for TLS1.2.
- Bouncy Castle – Crypto library used to validate OCSP only and no other verification of the TLS channel.
- Google Protobuf – Used for application-level messages (sent over the secure TLS channel).
- Google GSON – for non-network APIs/config requiring Json Parsing.
- Android end-user Application.
- SecureIO TLS 1.2
- SecureIO TCP
- Android TLS 1.2
- SSLContext

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 addressed the vulnerability analysis Assurance Activities in the SWAPP, 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 SWAPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The Validation team suggest 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 security functional requirements specified in the ST, 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

- [ST] *Perspecta Labs SecureIO v2.0.4 Security Target*, Version 0.8, June 30, 2021

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 1.3, dated, 01 March 2019 [SWAPP].
6. [ST] *Perspecta Labs SecureIO v2.0.4 Security Target*, Version 0.8, June 30, 2021.
7. [AGD] *Perspecta Labs SecureIO User Manual*, *Version 2.0.4*, Issue 6, June 2021.
8. [ETR] *Evaluation Technical Report for Perspecta Labs SecureIO v 2.0.4*, Version 0.2, June 2021.
9. [AAR] *Assurance Activity Report for Perspecta Labs SecureIO v2.0.4*, Version 0.2, June 30, 2021.
10. [DTR] *Test Plan for Perspecta Labs SecureIO v2.0.4 on Android 8*, Version 1.1, June 30, 2021.
11. [DTR] *Test Plan for Perspecta Labs SecureIO v2.0.4 on Android 9*, Version 1.1, June 30, 2021.
12. [DTR] *Test Plan for Perspecta Labs SecureIO v2.0.4 on Android 10*, Version 1.1, June 30, 2021.