National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Hypori Halo Client (Android) 4.3

Report Number: CCEVS-VR-VID11423-2024
Dated: 20 February 2024
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

Daniel Faigin

The Aerospace Corporation

Farid Ahmed

Russell Fink

Bryan Major

Michael Smeltzer

Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Hypori Halo Client (Android) 4.3 (the Target of Evaluation, or 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 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 in 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 evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. 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.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in December 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos. The evaluation determined that the TOE is:

- Common Criteria Part 2 Extended and Common Criteria Part 3 Extended

and demonstrates exact conformance to:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])

as clarified by all applicable Technical Decisions.

The TOE is Hypori Halo Client (Android) 4.3.

The TOE identified in this VR has been evaluated at a NIAP approved 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). 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 monitored the activities of the evaluation 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. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST ([6]).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 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 (PCL).

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

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules 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	Hypori Halo Client (Android) 4.3
Security Target	Hypori Halo Client (Android) 4.3 Security Target, Version 1.0, 15 February, 2024
Sponsor & Developer	Hypori, LLC. 1801 Robert Fulton Drive, Suite 440 Reston, VA 20191
Completion Date	February 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	Protection Profile for Application Software, Version 1.4, 7 October 2021
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046

Item	Identifier
Evaluation Personnel	Pascal Patin Allen Sant Josh Marciante Dawn Campbell
Validation Personnel	Daniel Faigin Farid Ahmed Russell Fink Bryan Major Michael Smeltzer

3 TOE Architecture

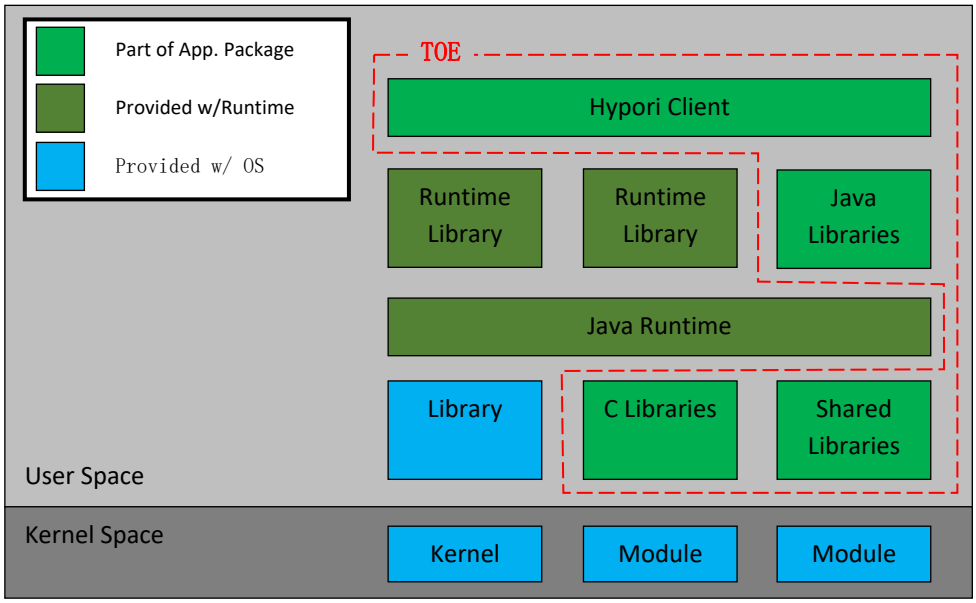
Note: The following architectural description is based on the description presented in the ST.

Hypori Halo Client (Android) 4.3 is a component of the Hypori Halo Platform. In the Hypori Halo platform, end users install and run the TOE on their mobile devices to access a Hypori Virtual Device running on a Hypori Server in the cloud. The Hypori Virtual Device on the Hypori Server contains data and applications for the users. The TOE communicates with the Hypori Virtual Device using TLS 1.2 and brokers access between the mobile device and the applications executing in the Hypori Virtual Device. This concept of operation is illustrated in the following figure.

Figure 1 Hypori Halo Client Communication with a Hypori Virtual Device on a Hypori Server

The TOE comprises the Hypori Halo Client (Android) 4.3 application that installs on the end user's mobile device and communicates with the Hypori Virtual Device on the server using TLS 1.2 (provided by the underlying Android platform). The Hypori Server, Hypori Virtual Device, Admin Console, applications running on the Hypori Server, the hardware platform device, and any functions not specified in the ST are outside the scope of the TOE. Figure 2 shows the relationship of the TOE to its operational environment.

Figure 2 TOE Boundary for Android Devices



The TOE's operational environment comprises the Android-based mobile device on which it is installed. The TOE is evaluated on Android releases 12 and 13.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Cryptographic Support

The TOE establishes secure communication with the Hypori Virtual Device on the server using TLS. It uses cryptographic services provided by the platform. The TOE stores credentials and certificates for mutual authentication in the platform's key chain.

4.2 User Data Protection

The TOE informs a user of hardware and software resources the TOE accesses. The user initiates a secure network connection to the Hypori Virtual Device on the server using the TOE. In general, sensitive data resides on the Hypori Server and not the TOE or TOE platform, although the TOE does store credentials as identified above in Section 4.1.

4.3 Identification and Authentication

The TOE supports X.509 certificate validation as part of establishing TLS connections. The TOE relies on platform-provided functionality to support certificate validity checking methods, including the checking of certificate revocation status using OCSP. If the validity status of a certificate cannot be determined, the certificate will not be accepted.

4.4 Security Management

Security management consists of setting Hypori Client configuration options and applying configuration policies from the Hypori Server. The TOE stores the configuration settings and policies encrypted using cryptographic services provided by the platform.

4.5 Privacy

The TOE does not transmit personally identifiable information (PII) over a network.

4.6 Protection of the TSF

The TOE uses security features and APIs that the platform provides. The TOE leverages package management for secure installation and updates. The TOE package includes only those third-party libraries necessary for its intended operation.

4.7 Trusted Path/Channels

The TOE invokes platform-provided functionality to encrypt all transmitted data using TLS 1.2 for all communication with the Hypori Virtual Device on the Hypori Server.

5 Assumptions and 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

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 evaluation activities specified in *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5]) and performed by the evaluation team).
- 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 Hypori Halo Client (Android) 4.3 Security Target, Version 1.0, 15 February, 2024 ([6]).
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in [6].
- This evaluation did not specifically search for, nor attempt to exploit, 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:

- *Hypori Halo Client User Guide, Common Criteria Configuration and Operation, Version 4.3* ([7])
- *Hypori Halo Administrator Guide, Version 1.18* ([8])

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 evaluation team. It is derived from information contained in the following proprietary document:

- *Hypori Halo Client (Android) 4.3 Common Criteria Test Report and Procedures,* Version 1.1, February 2, 2024 ([11])

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Hypori Halo Client (Android) 4.3*, Version 1.0, 2 February 2024 ([10])

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 *Protection Profile for Application Software* ([5]).

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Application Software*. 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 team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from July 24, 2023 to February 1, 2024.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Application Software* were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration consisting of the TOE (Hypori Halo Client (Android) 4.3) installed on each of the following Android devices:

- Google Pixel 6 running Android 12
- Samsung Galaxy 13 running Android 13.

The test configuration also included a test server and OCSP Responder used to support testing of X.509 requirements and a router used to run Wireshark captures and perform port scans. The test server, running Ubuntu 18.04, included the following testing tools:

- OpenSSL 1.1.1
- Custom Leidos CCTL TLS Server and Client test tools.

The router, running Ubuntu 22.04, included the following test tools:

- Nmap 7.8
- Wireshark 3.6.2.

8 Evaluated Configuration

The TOE consists of the Hypori Halo Client (Android) 4.3 software application, that communicates only with the Hypori Server in the Hypori Virtual Device on the Hypori server, using TLS 1.2 provided by the underlying Android platform.

The TOE is evaluated on Android 12 and 13.

The TOE imposes no hardware requirements beyond those of the Android operating system on which it is installed.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Hypori Halo Client (Android) 4.3 ([9]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5]). The evaluation determined the TOE satisfies the conformance claims made in the Hypori Halo Client (Android) 4.3 Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5]).

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

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

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV assurance 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 Protection Profile 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.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance assurance 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.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance 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 Protection Profile. 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.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_FUN.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.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance 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.

Searches of public vulnerability repositories were performed on October 24, 2023, December 22, 2023, on January 2, 2024, and on February 2, 2024.

The evaluation team searched the following public vulnerability repositories.

- National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search)
- US-CERT Vulnerability Notes Database (https://www.kb.cert.org/vuls/).

The evaluation team used the following search terms in the searches of these repositories:

- Hypori
- Hypori Client
- Hypori Halo
- Android Cloud Environment
- Thin Client
- Virtual Mobile Infrastructure
- Opus Audio Codec v1.1
- Protobuf v3.21.1
- Zxing core 3.3.0
- Yubikit v1.0.0
- AppAuth 0.9.1
- Moshi 1.13.0
- BouncyCastle 1.70
- Hasher 1.2
- Kotlin standard library 1.8.10
- kotlin-reflect 1.8.10
- kotlinx-coroutines 1.6.4
- Dagger Hilt v2.45.

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.

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 Protection Profile. Additionally, the evaluation team's testing 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 notes that the evaluated configuration was tested on two platforms: Google Pixel Phones running Android 12.0 and Samsung Galaxy Devices running Android 13. While the application may install and run on other platforms, no other platforms were evaluated. As a result, platform configurations and cryptographic support may differ and affect the behavior and cryptographic operations provided to the application.

The scope of this evaluation was limited to the functionality and assurances specified in the Security Target. Any other functionality provided in the environment and in the product itself was not assessed as part of this evaluation. Environment components not part of the evaluation include any virtual Android devices running on a server in the cloud. Any additional functionality provided by other devices in the operational environment need to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance and they should follow any configuration instructions provided for the platform as described in the platform's Configuration Guidance documentation.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Security Target

The ST for this product's evaluation is *Hypori Halo Client (Android) 4.3 Security Target, Version 1.0, 15 February, 2024* [6].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PII	Personally Identifiable Information
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VMI	Virtual Mobile Infrastructure
VR	Validation Report

13 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, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, 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, April 2017.

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

[5] Protection Profile for Application Software, Version 1.4, 7 October 2021.

[6] Hypori Halo Client (Android) 4.3 Security Target, Version 1.0, 15 February, 2024.

[7] Halo Client User Guide, Common Criteria Configuration and Operation, Version 4.3

[8] Hypori Halo Administrator Guide, Version 1.18

[9] Evaluation Technical Report for Hypori Halo Client (Android) 4.3 (Proprietary), Version 1.0, 2 February 2024.

[10] Assurance Activities Report for Hypori Halo Client (Android) 4.3, Version 1.0, 2 February 2024.

[11] Hypori Halo Client (Android) 4.3 Common Criteria Test Report and Procedures, Version 1.1, 2 February, 2024.