National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

for

Intelligent Waves Virtual Mobile Infrastructure Platform 4.1 Hypori Client for Android

Report Number: CCEVS-VR-10874-2018
Dated: August 24, 2018
Version: 1.0

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

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

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report 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 Application Software in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 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 Hypori Client (Android) 4.1. It presents the evaluation results, their justifications, and the conformance results. The Target of Evaluation (TOE) is the Hypori Client (Android) 4.1. 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 as documented in the ST.

The evaluation of the Hypori Client (Android) 4.1 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in August 2018. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in *Protection Profile for Application Software*, Version 1.2, 22 April 2016 (PP APP SW) including *DoD Annex for Protection Profile for Application Software v1.2*, Version 1 Release 1, 21 February 2018. The following NIAP Technical Decisions apply to evaluation assurance activities.

- TD0107: FCS_CKM - ANSI X9.31-1998, Section 4.1 for Cryptographic Key Generation
- TD0119: FCS_STO_EXT.1.1 in PP_APP_v1.2
- TD0163: Update to FCS_TLSC_EXT.1.1 Test 5.4 and FCS_TLSS_EXT.1.1 Test
- TD0172: Additional APIs added to FCS_RBG_EXT.1.1
- TD0174: Optional Ciphersuites for TLS
- TD0178: Integrity for installation tests in AppSW PP
- TD0192: Update to FCS_STO_EXT.1 Application Note
- TD0217: Compliance to RFC5759 and RFC5280 for using CRLs
- TD0221: FMT_SMF.1.1 Assignments moved to Selections
- TD0238: User-modifiable files FTP_AEX_EXT.1.4
- TD0244: FCS_TLSC_EXT - TLS Client Curves Allowed
- TD0268: FMT_MEC_EXT.1 Clarification
- TD0283: Cipher Suites for TLS in SWApp v1.2
- TD0295: Update to FPT_AEX_EXT.1.3 Assurance Activities
- TD0300: Sensitive Data in FDP_DAR_EXT.1
- TD0304: Update to FCS_TLSC_EXT.1.2
- TD0305: Handling of TLS connections with and without mutual authentication
- TD0327: Default file permissions for FMT_CFG_EXT.1.2

The following NIAP Technical Decisions are associated with the claimed PP but were not included in the Security Target. The following Technical Decisions identify Security Functional Requirements that are not identified in the Security Target

- TD0121: FMT_MEC_EXT.1.1 Configuration Options
  - The TD is not applicable to the TOE. The TD is only applicable when a TOE is claiming compliance to the SWFE EP
- TD0131: Update to FCS_TLSS_EXT.1.1 Test 4.5
  - The TD is not applicable to the TOE. The TOE is a TLS Client.
- TD0177: FCS_TLSS_EXT.1 Application Note Update
  - The TD is not applicable to the TOE. The TOE is a TLS Client.
- TD0215: Update to FCS_HTTPS_EXT.1.2
  - The TD is not applicable to the TOE. The TOE does not claim HTTPS.
- TD0241: Removal of Test 4.1 in FCS_TLSS_EXT.1.1
  - The TD is not applicable to the TOE. The TOE is a TLS Client.
- TD0267: TLSS testing - Empty Certificate Authorities list
  - The TD is not applicable to the TOE. The TOE is a TLS Client.
- TD0296: Update to FCS_HTTPS_EXT.1.3
  - The TD is not applicable to the TOE. The TOE does not claim HTTPS.
- TD0326: RSA-based key establishment schemes
  - This TD is not applicable to the TOE. The TOE does not claim FCS_CKM.1, FCS_CKM.2, or FCS_TLSS_EXT.1.3

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the Hypori Client (Android) 4.1 is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

The TOE is a software application that consists of the Hypori Client (Android) 4.1 that runs on Android versions 5.0, 5.1, 6.0, 7.0, and 7.1.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. Therefore 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 (ETR) are consistent with the evidence produced.

The technical information included in this report was obtained from the Intelligent Waves Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Security Target, version 4.1, August 2, 2018 and analysis performed by the Validation Team.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Hypori Client (Android) 4.1
Sponsor & Developer	Intelligent Waves, LLC. 1801 Robert Fulton Drive, Suite 440 Reston, VA 20191 United States
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	August 2018
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	*Protection Profile for Application Software,* Version 1.2, 22 April 2016 (PP APP SW) including *DoD Annex for Protection Profile for Application Software v1.2*, Version 1 Release 1, 21 February 2018 and the NIAP Technical Decisions referenced in Section 1 of this VR.
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the Hypori Client (Android) 4.1
Evaluation Personnel	Greg Beaver Cody Cummins Pascal Patin *Leidos*
Validation Personnel	Daniel Faigin Meredith Hennan *The Aerospace Corporation*

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) 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 Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Intelligent Waves Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Security Target
ST Version	4.1
Publication Date	August 2, 2018
Vendor	Intelligent Waves, LLC
ST Author	Intelligent Waves, LLC
TOE Reference	Hypori Client (Android) 4.1
TOE Software Version	Hypori Client (Android) 4.1
Keywords	Virtual Mobile Infrastructure, Android Cloud Environment Component, Thin Client

2.1 Threats

The ST references the *Protection Profile for Application Software*, Version 1.2, 22 April 2016 including the *DoD Annex for Protection Profile for Application Software v1.2*, Version 1 Release 1, 21 February 2018.

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
- An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
- An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.

- An attacker may try to access sensitive data at rest.

2.2 Organizational Security Policies

There are no OSPs for the application.

3 Architectural Information

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

The TOE is the Android-based Hypori Client. Figure 1 shows how the TOE interacts with a Hypori Device running applications on a Hypori Server. The Hypori Client is a thin client that communicates only with a Hypori Virtual Device on a Hypori Server and not with other servers or applications.

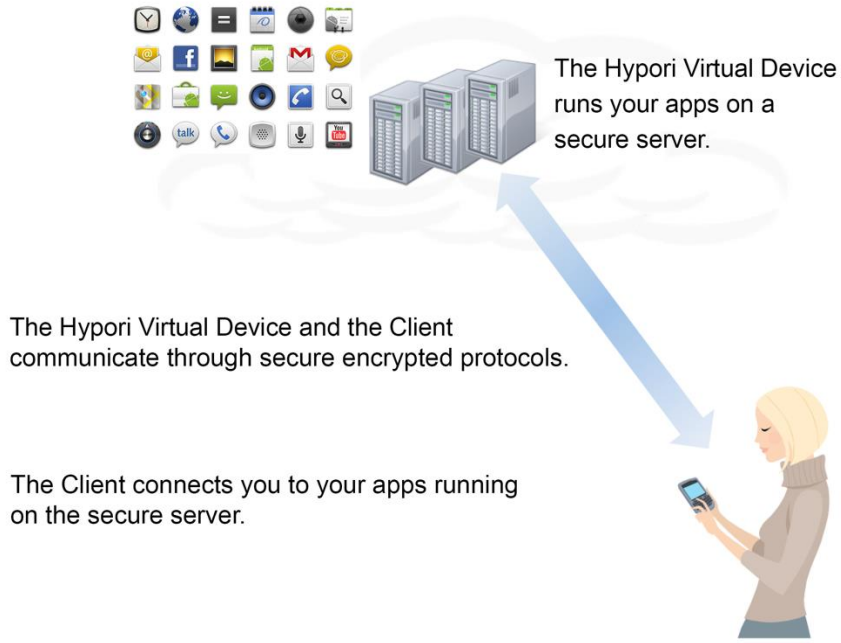

Figure 1 Hypori Client as Part of VMI Platform

3.1 TOE Architecture

The section describes the TOE architecture including physical and logical boundaries. Figure 2 shows the relationship of the TOE to its operational environment along with the TOE boundary. The security functional requirements identify the libraries included in the application package.

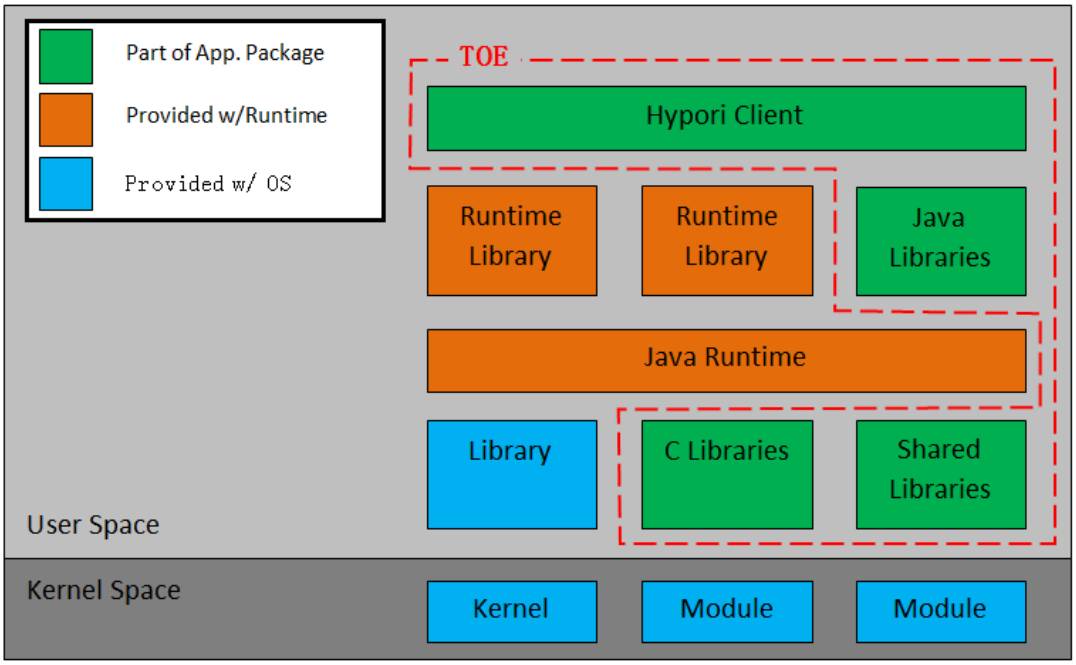

Figure 2 TOE Boundary

The TOE consists of a Hypori Client application as defined in the Hypori Client installation package. The TOE runs on Android versions 5.0, 5.1, 6.0, 7.0, and 7.1. The TOE imposes no hardware requirements beyond Android operating system requirements.

3.2 Physical Boundaries

The TOE consists of a Hypori Client application as defined in the Hypori Client installation package. The Hypori Client is an Android-based thin client that only communicates with the Hypori server. The Hypori server, applications running on the Hypori server, and any functions not specified in this security target are outside the scope of the TOE.

3.2.1 Software Requirements

The TOE runs on Android versions 5.0, 5.1, 6.0, 7.0, and 7.1.

3.2.2 Hardware Requirements

The TOE imposes no hardware requirements beyond Android operating system requirements.

4 Assumptions

The ST references the *Protection Profile for Application Software,* Version 1.2, 22 April 2016 including the *DoD Annex for Protection Profile for Application Software v1.2,* Version 1 Release 1, 21 February 2018. to identify following assumptions about the use of the product:

- The TOE relies upon a trustworthy computing platform 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 within compliance of the applied enterprise security policy.

4.1 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.
5. The TOE can be configured to rely on and utilize a number of other components in its operational environment:
    a. Hypori Virtual Device: This is an Android-based virtualized mobile device executing on a server in the cloud.
    b. Hypori Servers: This is the cloud server cluster that hosts the Hypori Virtual Devices.
    c. Hypori Admin Console: This is a browser-based administration user interface that is used to manage the Hypori system.

5 Security Policy

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

5.1 Cryptographic Support

The TOE establishes secure communication with the Hypori server using TLS. The client uses cryptographic services provided by the platform. TOE stores credentials and certificates for mutual authentication in the platform's keychain.

5.2 User Data Protection

The TOE informs a user of hardware and software resources the TOE accesses. It uses the platform's permission mechanism to get a user's approval for access as part of the installation process. The user initiates a secure network connection to the Hypori server using the TOE. In general, sensitive data resides on the Hypori server and not the Hypori Client, although the client does store credentials in the Android key store.

5.3 Identification and Authentication

The TOE uses the Android certification validation services to authenticate the X.509 certificate the Hypori Server presents as part of the establishing a TLS connection.

5.4 Security Management

Security management consists of setting Hypori Client configuration options. The TOE uses Android mechanisms for storing the configuration settings.

5.5 Privacy

The TOE does not transmit PII over a network.

5.6 Protection of the TSF

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

5.7 Trusted Path/Channels

TOE uses TLS 1.2 for all communication with Hypori Server.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, the following Common Criteria specific guide references the security-related guidance material for the software in the evaluated configuration:

- Hypori User Guide Common Criteria Configuration and Operation, Version 4.1
- Hypori User Guide, Version 4.1.0

To use the product in the evaluated configuration, the product must be configured as specified in the Common Criteria Configuration and Operation guide. 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 device as evaluated.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Hypori Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Common Criteria Test Report and Procedures, Version 1.0, August 3, 2018

The test results are recorded in the publicly available Hypori Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Common Criteria Assurance Activities Report, Version 1.2, August 3, 2018.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities of this product.

7.2 Evaluation Team Independent Testing

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the *Protection Profile for Application Software*, Version 1.2, 22 April 2016 including the *DoD Annex for Protection Profile for Application Software v1.2*, Version 1 Release 1, 21 February 2018 and the applicable NIAP Technical Decisions referenced in section 1 of this VR.

To this end, the evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the above-referenced Protection Profile.

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 the Leidos facility in Columbia, Maryland from November 1, 2017 through August 3, 2018.

7.3 Test Configuration

The evaluators received the TOE in the form that normal 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. As can be seen in Figure 3 below, the configuration used during testing of the TOE matches that which was defined in the Security Target.

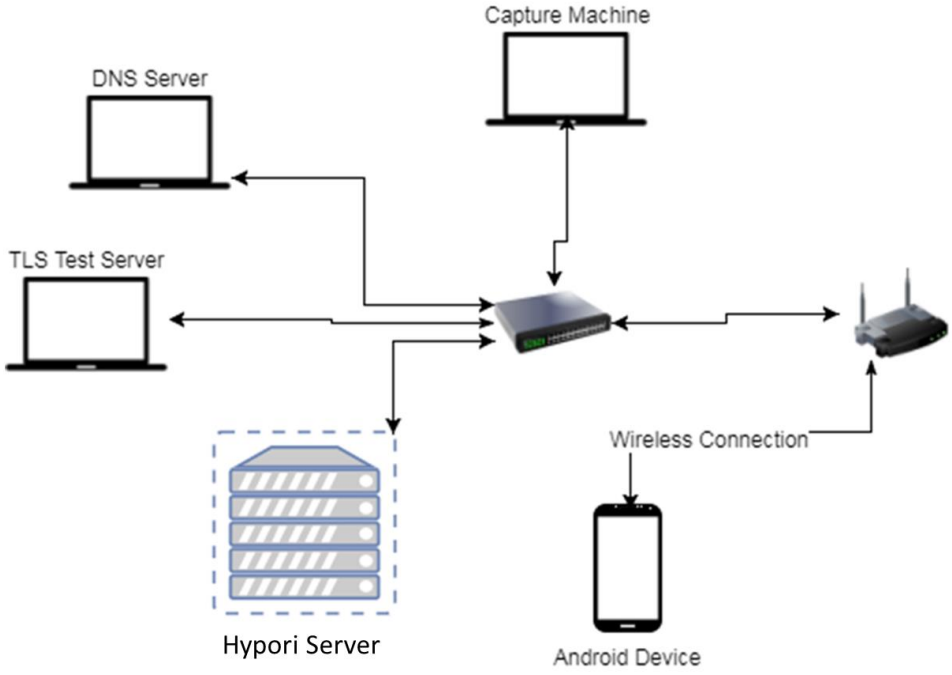

Figure 3 Test Configuration

As documented in the diagram above, the following hardware and software components were included in the evaluated configuration during testing:

TOE

- Hypori Client App deployed on Nexus 5x running Android 7.1.2
- Hypori Client App deployed on Samsung Galaxy Tab S2 running Android 6.0.1
- Hypori Client App deployed on LG G Tab running Android 5.0.2

Additional Components

- ESXI Server running the Hypori ACE Server components
- DNS server running on Windows Server 2012
- Windows machine to capture network packets using mirrored switch
- Linux Machine running the NIAP provided TLS test server tool
- The Common Criteria/ TLS-CC-Tool for testing TLS in NIAP's Application Software Protection Profile.

The Common Criteria/ TLS-CC-Tool is suitable for manipulating individual fields within TLS packets, as specified in the Test Assurance Activities. The Test Tool can be downloaded at https://github.com/commoncriteria/tls-cc-tools.

The configuration used during testing of the TOE matches that which was defined in the Security Target.

The evaluated version of the TOE was installed and configured according to the *Hypori User Guide Common Criteria Configuration and Operation*, Version 4.1 as well as the supporting guidance documentation identified in Section 6.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the *Protection Profile for Application Software*, Version 1.2, 22 April 2016 including the *DoD Annex for Protection Profile for Application Software v1.2*, Version 1 Release 1, 21 February 2018 are fulfilled.

7.4 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration. A virus scan against the application was executed using the McAfee VirusScan Enterprise + AntiSpyware Enterprise 10.5.

8 Evaluated Configuration

The TOE Evaluated Configuration is the Hypori Client application version 4.1 running on Android version 5.0, 5.1, 6.0, 7.0, or 7.1.

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 ETR. All assurance activities and work units received a passing verdict.

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Application Software*, Version 1.2, 22 April 2016 (including all supplementary materials published by NIAP) as well as the Common Evaluation Methodology (CEM) for Version 3.1 revision 4 of the Common Criteria, to which the claimed PP claims conformance.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. All work units passed and all evaluation assurance activities were completed successfully.

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 claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are detailed in the following sections.

9.1 Evaluation of the Security Target (ASE)

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 TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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 the Development (ADV)

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 and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the PP related to the examination of the information contained in the TSS.

The validators 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.

9.3 Evaluation of the Guidance Documents (AGD)

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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators 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.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

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

The validators 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 the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the PP and recorded the results in a Test Report, as characterized in the AAR.

The validators 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 (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability assessment analysis is identified in the Hypori Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Common Criteria Test Report and Procedures, Version 1.0, August 3, 2018. The vulnerability assessment was performed on July 30, 2018. No vulnerabilities were identified in the search of public information. No vulnerabilities were identified as a result of the virus scan.

Open source information was examined to ensure the vulnerability analysis did not miss any well-known vulnerability.

The http://web.nvd.nist.gov/view/vuln/search web site to ensure that all vulnerabilities pertaining to the TOE have been addressed. The search was conducted using the following terms:

- Hypori
- Intelligent Waves
- Virtual Mobile Infrastructure
- Hypori Client
- Cloud
- Android Cloud Environment
- Android Cloud
- Thin Client
- Spectre
- Meltdown

A virus scan was executed against the TOE application files. The virus scanner used was the McAfee Endpoint Security 10.5, updated on May 17, 2018. The virus scan was performed on the day of the update. No virus or malware was detected.

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 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

All validator comments have been addressed in the Clarification of Scope section.

11 Annexes

Not applicable

12 Security Target

- Intelligent Waves Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Security Target, August 2, 2018

13 Abbreviations and Acronyms

Abbreviation	Description
API	Application Programming Interface
App	Software application
ASLR	Address Space Layout Randomization
CC	Common Criteria
CEM	Common Evaluation Methodology
DEP	Data Execution Prevention
DoD	Department of Defense
OS	Operating System
PII	Personally Identifiable Information
PP	Protection Profile
PP APP SW	Protection Profile for Application Software
SAR	Security assurance requirement
SFR	Security functional requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
VMI	Virtual Mobile Infrastructure

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, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[6] Intelligent Waves Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Security Target, August 2, 2018

[7] Hypori Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Common Criteria Test Report and Procedures, Version 1.0, August 3, 2018

[8] Hypori Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Common Criteria Assurance Activities Report, Version 1.2, August 3, 2018

[9] Hypori User Guide Common Criteria Configuration and Operation, Version 4.1

[10] Evaluation Technical Report For Hypori Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Part 1 Non-Proprietary, Version 1.0, August 3, 2018

[11] Evaluation Technical Report For Hypori Virtual Mobile Infrastructure Platform 4.1 Hypori Client (Android) Part 2 Hypori Proprietary, Version 0.5, August 3, 2018