National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Hypori Android Cloud Environment Client 3.1.0

Report Number: CCEVS-VR-10643-2016
Dated: March 9, 2016
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 documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Hypori Android Cloud Environment Client 3.1.0 (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 applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

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.

The evaluation of the Hypori Android Cloud Environment Client 3.1.0 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in February 2016. 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 1.1, 5 November 2014 (PP APP SW) including *DoD Annex for Protection Profile for Application Software* v1.0, Version 1, Release 1 (DoD Annex), 22 October 2014. NIAP Technical Decision TD0051 Android Implementation of TLS in App PP v1.1 applies and is addressed in this VR. The following NIAP Technical Decisions apply to evaluation assurance activities.

- TD0054: Clarification of FPT_API_EXT.1.1 Requirement in APP PP v1.1
- TD0050: FMT_CFG_EXT.1.2 Change in APP SW PPv1.1.

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 Android Cloud Environment Client 3.1.0 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 Android Cloud Environment Client 3.1.0 that runs on Android versions 4.3, 4.4, 5.0 and 5.1.

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 are consistent with the evidence produced.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Hypori Android Cloud Environment Client 3.1.0

Item	Identifier
Sponsor & Developer	Hypori, Inc. 9211 Waterford Centre Blvd, Suite 100 Austin, TX 78758 United States
CCTL	Leidos (formerly SAIC) Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	February 2016
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 1.1, 5 November 2014 (PP APP SW) including *DoD Annex for Protection Profile for Application Software* v1.0, Version 1, Release 1 (DoD Annex), 22 October 2014. NIAP Technical Decision TD0051 Android Implementation of TLS in App PP v1.1 applies and is addressed in this ST. The following NIAP Technical Decisions apply to evaluation assurance activities. • TD0054: Clarification of FPT_API_EXT.1.1 Requirement in APP PP v1.1 • TD0050: FMT_CFG_EXT.1.2 Change in APP SW PPv1.1.
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the Hypori Android Cloud Environment Client 3.1.0
Evaluation Personnel	Leidos (formerly SAIC): Greg Beaver Cody Cummins Tony Apted
Validation Body	National Information Assurance Partnership CCEVS
Validation Personnel	Daniel Faigin, The Aerospace Corporation Ken Stutterheim, The Aerospace Corporation 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	Hypori Virtual Mobile Infrastructure Platform 3.1.0 Android Cloud Environment Client Security Target
ST Version	1.0
Publication Date	February 17, 2016
Vendor	Hypori, Inc.
ST Author	Leidos (formerly SAIC)
TOE Reference	Hypori Android Cloud Environment Client 3.1.0
TOE Software Version	Hypori Android Cloud Environment Client 3.1.0
Keywords	Virtual Mobile Infrastructure, Android Cloud Environment Component, Thin Client

2.1 Threats

The ST references the *Protection Profile for Application Software*, Version 1.1, 5 November 2014 (PP APP SW) including *DoD Annex for Protection Profile for Application Software* v1.0, Version 1, Release 1 (DoD Annex), 22 October 2014. NIAP Technical Decision TD0051 Android Implementation of TLS in App PP v1.1 applies and is addressed in this ST. The following NIAP Technical Decisions apply to evaluation assurance activities.

- TD0054: Clarification of FPT_API_EXT.1.1 Requirement in APP PP v1.1
- TD0050: FMT_CFG_EXT.1.2 Change in APP SW PPv1.1.

to identify 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

3.1 TOE Introduction

The TOE is the Hypori ACE Client. The following diagram shows how the TOE interacts with an ACE Device running applications on an ACE Server. An ACE Client is a thin client that communicates only with an ACE Device on an ACE Server and not with other servers or applications.

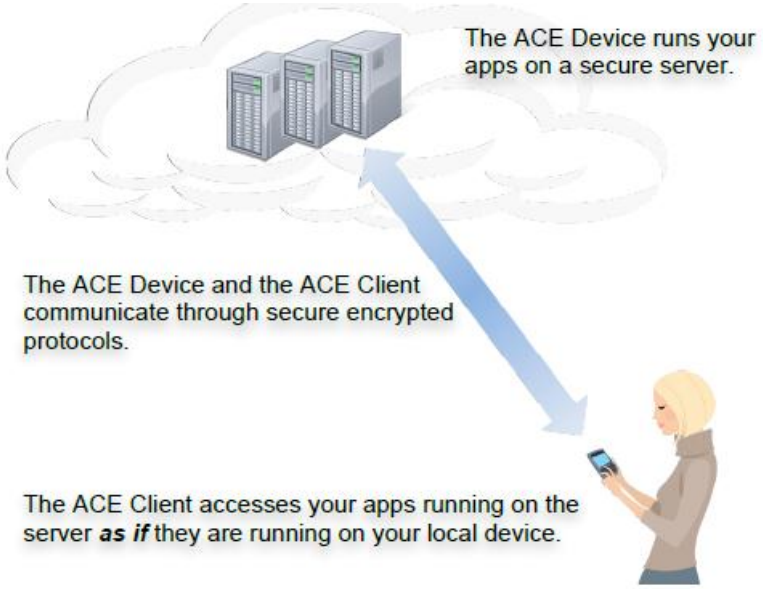


Figure 1 ACE Client as Part of VMI Platform

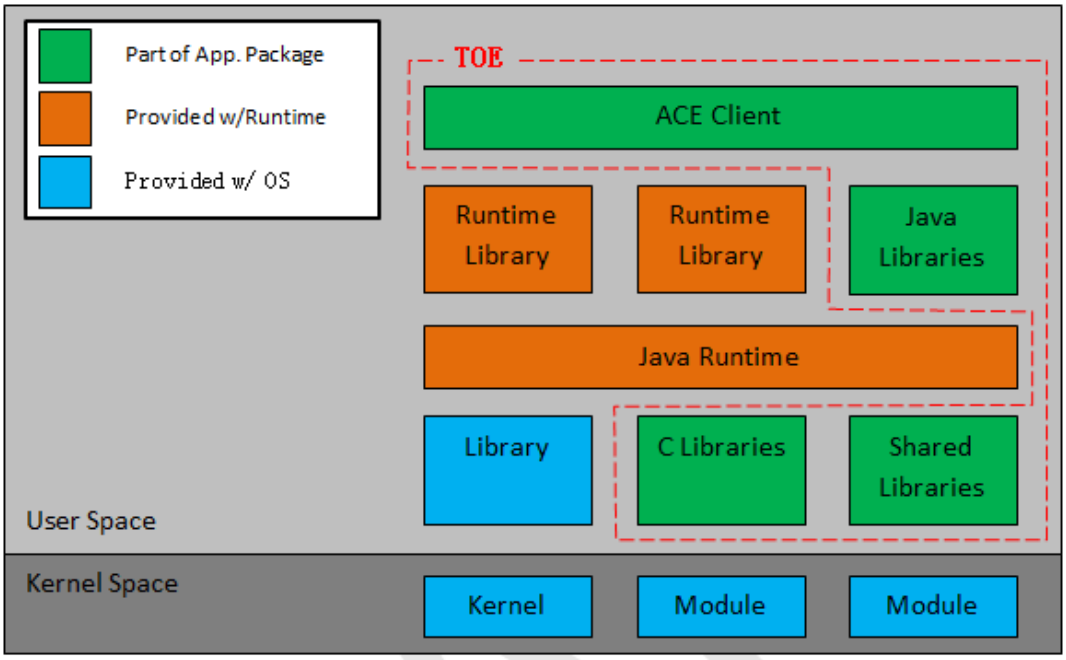
3.2 TOE Evaluated Configuration

The TOE evaluated configuration is the Android Cloud Environment Client component of the Virtual Mobile Infrastructure Platform version 3.1.0 provided by Hypori, Inc. for Android versions 4.3, 4.4, 5.0 and 5.1.

3.3 Physical Boundaries

The section describes the physical boundaries of the TOE architecture. Figure 1 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 ACE Client application and configuration settings as defined in the ACE Client installation package for Android. The TOE runs on Android versions 4.3, 4.4, 5.0 and 5.1. The TOE imposes no hardware requirements beyond Android operating system requirements.

4 Security Policy

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

1. Cryptographic Support
2. User Data Protection
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. Trusted Path/Channels

4.1 Cryptographic Support

The TOE establishes secure communication with the ACE Server using TLS. The client uses cryptographic services provided by the Android platform. TOE stores credentials and certificates for mutual authentication in the Android key store.

4.2 User Data Protection

The TOE informs a user of hardware and software resources the TOE accesses. It uses the Android 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 ACE Server using the TOE. In general, sensitive data resides on the ACE Device and not the ACE Client, although the client does store credentials in the Android key store.

4.3 Identification and Authentication

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

4.4 Security Management

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

4.5 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.

4.6 Trusted Path/Channels

TOE uses TLS 1.2 for all communication with ACE Server.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the Protection Profile for Application Software, Version 1.1, 5 November 2014 (PP APP SW) including DoD Annex for Protection Profile for Application Software v1.0, Version 1, Release 1 (DoD Annex), 22 October 2014 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.

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:

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. ACE Device: This is an Android-based virtualized version of the end user's mobile device.
    b. ACE Servers: This is the cloud server cluster that hosts the ACE Devices.
    c. ACE Administrator Portal: This is a browser-based administration user interface that is used to manage the ACE system.
6. The functionality evaluated is scoped exclusively to the security functional requirements specified in the PP APP SW. Any additional security related functional capabilities of the TOE are not covered by this evaluation.

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 ACE User Guide Common Criteria Configuration and Operation - Version 3.1.0
- Hypori ACE Client Install Guide for Android Devices, Version 3.1 - Enterprise Distribution
- Hypori ACE User Guide for Android Devices, Version 3.1 - ACE Device

Supporting TOE Guidance Documentation

- Hypori Virtual Mobile Infrastructure Platform 3.1.0 Android Cloud Environment Client Security Target, Version 1.0, February 17, 2016

7 IT Product Testing

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

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

- Evaluation Team Hypori Virtual Mobile Infrastructure Platform 3.1.0 Android Cloud Environment Client Common Criteria Test Report and Procedures, Version 1.0, Feb 17 2016

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 1.1, 5 November 2014 (PP APP SW) including *DoD Annex for Protection Profile for Application Software* v1.0, Version 1, Release 1 (DoD Annex), 22 October 2014. NIAP Technical Decision TD0051 Android Implementation of TLS in App PP v1.1 applies and is addressed in this ST. The following NIAP Technical Decisions apply to evaluation assurance activities.

- TD0054: Clarification of FPT_API_EXT.1.1 Requirement in APP PP v1.1
- TD0050: FMT_CFG_EXT.1.2 Change in APP SW PPv1.1.

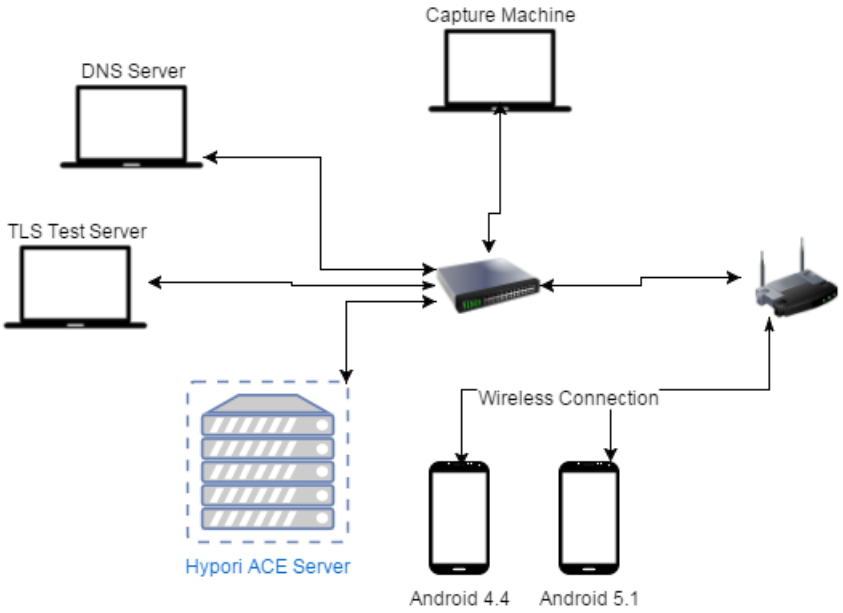
To this end, the evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the above-referenced Protection Profile.

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 December 1, 2015 – February 15, 2016.

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 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

- ACE Client App deployed on Samsung Galaxy S6 running Android 5.1
- ACE Client App deployed on Samsung Galaxy S5 running Android 4.4

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 ACE User Guide Common Criteria Configuration and Operation*, Version 3.1.0 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 1.1, 5 November 2014 (PP APP SW) including *DoD Annex for Protection Profile for Application Software* v1.0, Version 1, Release 1 (DoD Annex), 22 October 2014 are fulfilled.

7.3 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 8.8.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Application Software,* Version 1.1, 5 November 2014 (PP APP SW) including *DoD Annex for Protection Profile for Application Software* v1.0, Version 1, Release 1 (DoD Annex), 22 October 2014.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

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 listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ALC_TSU_EXT.1	ALC_TSU_EXT.1 Timely Security Updates
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

All validator comments are addressed in the Clarification of Scope section.

10 Annexes

Not applicable

11 Security Target

- Hypori Virtual Mobile Infrastructure Platform 3.1.0 Android Cloud Environment Client Security Target, Version 1.0, February 17, 2016

12 Abbreviations and Acronyms

Abbreviation	Description
ACE	Android Cloud Environment
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

13 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] Hypori Virtual Mobile Infrastructure Platform 3.1.0 Android Cloud Environment Client Security Target, Version 1.0, February 17, 2016

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

[7] Evaluation Team Hypori Virtual Mobile Infrastructure Platform 3.1.0 Android Cloud Environment Client Common Criteria Test Report and Procedures, Version 1.0, Feb 17 2016