National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Cog Systems

Level 1, 277 King Street

Newtown NSW 2042 Australia

HTC A9 Secured by Cog Systems D4

Report Number: CCEVS-VR-VID10776-2017
Dated: May 25, 2017
Version: 0.3

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

ACKNOWLEDGEMENTS

Validation Team

Stelios Melachrinoudis
The MITRE Corporation

Marybeth Panock
Kenneth Stutterheim
The Aerospace Corporation

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team for the evaluation of the HTC A9, Secured by Cog Systems D4 solution provided by Cog Systems. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in May 2017. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. That information is summarized in the Assurance Activity Report (MDFPP20) For HTC A9 Secured By COG Systems D4 (AAR). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the Protection Profile For Mobile Device Fundamentals, Version 2.0, 17 September 2014.

The Target of Evaluation (TOE) is the HTC A9, Secured by Cog Systems D4, and the associated TOE guidance documentation.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report 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 and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (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.

The technical information included in this report was obtained from the HTC A9, Secured by Cog Systems D4 (MDFPP20) Security Target, version 0.5, May 12, 2017 and the analysis of the evaluation evidence as 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile 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	HTC A9, Secured by Cog Systems D4
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 2.0, 17 September 2014
ST	HTC A9, Secured by Cog Systems D4 Security Target, version 0.5, May 12, 2017
Evaluation Technical Report	Evaluation Technical Report for HTC A9, Secured by Cog Systems D4, version 0.2, May 12, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cog Systems
Developer	Cog Systems
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Stelios Melachrinoudis, The MITRE Corporation

Item	Identifier
	Marybeth Panock, Kenneth Stutterheim, The Aerospace Corporation

3 Architectural Information

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

The Target of Evaluation is the D4 Secure Mobile device. The D4 Secure is a smartphone based upon HTC A9 hardware which uses Qualcomm System on a Chip (SoC) (Snapdragon 617, MSM8952). This is a custom built smartphone intended to support military and civil service users.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of one D4 Secure Mobile device.

Product	Security SW Version	OS Version	HTC Software Version Number
HTC-A9	0.3	Android v6.0.1	1.57.617.52

3.2 TOE Architecture

The TOE utilizes an OKL4 separation kernel (hypervisor), to provide 'cells' (i.e., a virtualized environment) that virtualize and isolate different aspects of the phone's hardware. The TOE includes the Qualcomm Secure Execution Environment (QSEE) Trustzone, the separation kernel/hypervisor, custom D4 Secure Mobile 'cells' and a high-level operating system, along with the HTC A9 hardware. While the D4 Secure Mobile can support any operating system, the high level OS included in this evaluation is Android version 6.0.1.

The HTC A9 hardware is based upon the Qualcomm Snapdragon 617, MSM 8952 SoC. The SoC includes a Qualcomm Integrated Cryptographic Engine (ICE) to perform encryption and decryption operations with hardware implemented AES algorithm and software configured keys.

The TOE's Android cell includes a high-level OS. This high-level OS is a full implementation of Android 6.0.1, modified as necessary to satisfy MDFPP20 requirements. The Android cell provides an Application Programming Interface to mobile applications and provides users installing an application with the ability to either approve or reject an

application based upon the API access that the application requires. The Android cell provides many (but not all) of the TOE security functions required by the MDFPP20.

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are intended to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

The TOE's physical boundary is the physical perimeter of the mobile device enclosure.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security Management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Cryptographic support

The TOE includes multiple instances of the OpenSSL cryptographic library with CAVP validated algorithms to support cryptographic functions including: asymmetric key generation and establishment, symmetric key generation, encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key and protected data destruction. These primitive cryptographic functions are used to implement security protocols such as TLS and HTTPS and also to encrypt the media (including the generation and protection of data, keys, and key encryption keys) used by the TOE. Many of these cryptographic functions are also accessible as services to applications running on the TOE.

4.2 User data protection

The TOE controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE protects user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected.

4.3 Identification and authentication

The TOE supports features related to identification and authentication. From a user perspective, except for limited functionality such as making phone calls to an emergency number and receiving notifications, a password (i.e., Password Authentication Factor) must be correctly entered to unlock the TOE. Also, even when the TOE is unlocked the password must be re-entered to change the password. Passwords are obscured when entered so they cannot be read from the TOE's display. The TOE limits the frequency of password entry such that when a configured number of failures occurs, the TOE performs a full wipe of protected content. Passwords can be constructed using upper and lower case characters, numbers, and special characters. Passwords up to 14 characters in length are supported.

The TOE serves as an IEEE 802.1X supplicant and can use X509v3 certificates and perform certificate validation for a number of functions such as EAP-TLS, TLS, and HTTPS exchanges.

4.4 Security management

The TOE provides the interfaces necessary to manage the security functions claimed in the corresponding Security Target (and conforming to the MDFPP requirements) as well as other functions that might be commonly found in mobile devices.

4.5 Protection of the TSF

The TOE implements features to protect itself to ensure the reliability and integrity of its security features. It protects sensitive data such as cryptographic keys so that they are not accessible or exportable. It has access to a timing mechanism to ensure that reliable time information is available (e.g., for cryptographic operations). It enforces read, write, and execute memory page protections, uses address space layout randomization and stack-based buffer overflow protections to minimize the potential to exploit application flaws. Those features help to protect the TOE from modification by applications as well as to isolate the address spaces of applications from one another to protect those applications. The TOE employs a Secure Boot process that uses cryptographic signatures to ensure the authenticity and integrity of the bootloader, and the secure boot partition produced by Cog. The cryptographic signatures utilize data fused into the device processor.

The TOE includes functions to perform self-tests and software/firmware integrity checking so that it might detect if it is failing or is corrupt. If any self-test fails, the TOE will not enter an operational mode. The TOE also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation.

4.6 TOE access

The TOE can be locked, either by a user or after a configured interval of inactivity, thereby obscuring its display. The TOE has the capability to display an advisory message (banner) when users unlock the TOE for use.

The TOE is able to attempt to connect to wireless networks as configured.

4.7 Trusted path/channels

The TOE supports the use of IEEE 802.11-2012, IEEE 802.1X, and/or EAP-TLS to secure communications channels between itself and other trusted network devices.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile For Mobile Device Fundamentals, Version 2.0, 17 September 2014

That information has not been reproduced here and the MDFPP20 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the MDFPP20 as described for this TOE in the Security Target. 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 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 assurance activities specified in the Mobile Device Fundamentals Protection Profile and performed by the evaluation team).
- This evaluation covers only the specific device model and software as identified in this document, and not any earlier or later versions released or in process.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the MDFPP20 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- HTC A9, Secured By D4 Administrator Guide Instructions, Version 0.34, 6 March 2017

Any additional customer documentation provided with the product, or that is available on-line was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

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 proprietary Detailed Test Report (MDFPP20) for HTC A9, Secured by Cog Systems D4, Version 0.2, May 12, 2017 (DTR) and as summarized in the publically available Assurance Activity Report (MDFPP20) for HTC A9 Secured by COG Systems D4, Version 0.3, 5.19.17 (AAR).

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 Common Criteria Certification documents and ran the tests specified in the MDFPP20 including the tests associated with optional requirements.

8.3 Test Environment

The following diagrams depict the test environments used by the evaluators.

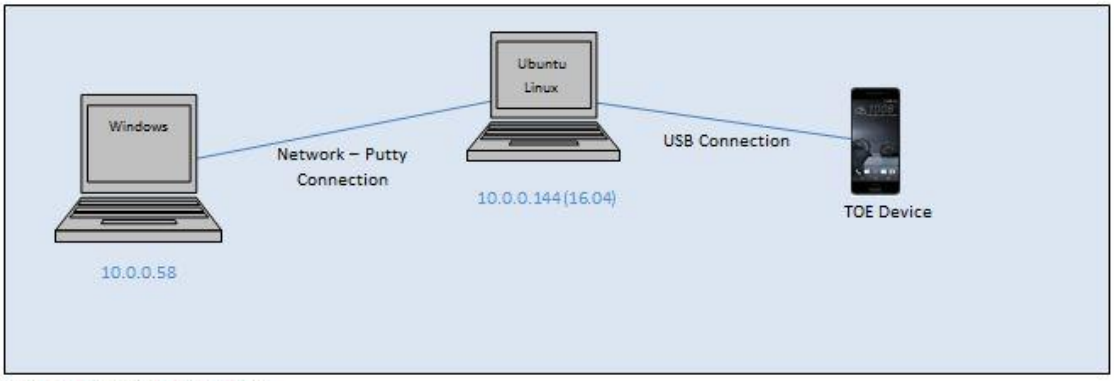

Figure 1 Evaluator Test Setup 1

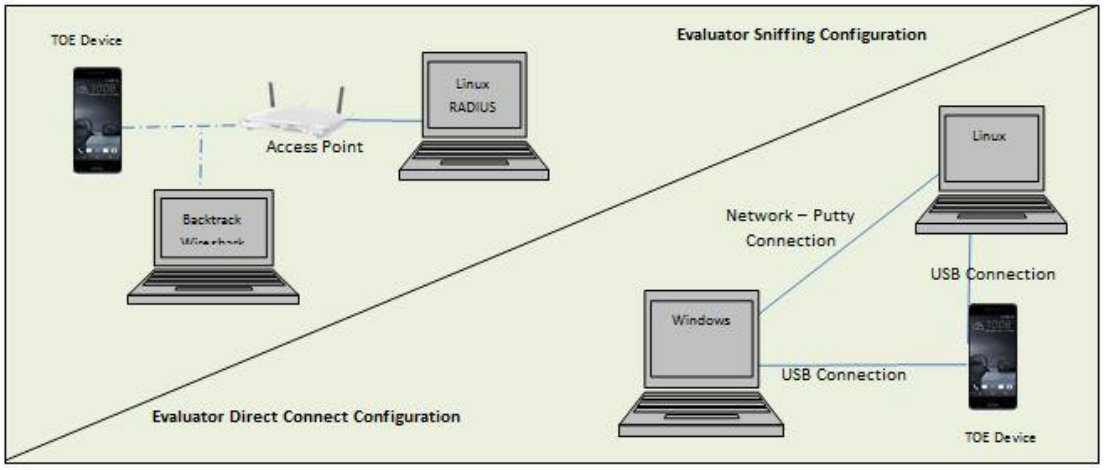

Figure 2 Evaluator Test Setup 2

9 Evaluated Configuration

The evaluated configuration consists of one D4 Secure smartphone based upon HTC A9 hardware which uses Qualcomm SoCs (Snapdragon 617, MSM8952). The product must be configured as specified in the HTC A9, Secured by Cog Systems D4 Adminstrator Guide Instructions, 6 March 2017, version 0.34.

10 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. The reader of this document can assume that all assurance 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 4 and CEM version 3.1 rev 4. The evaluation determined the HTC A9, Secured by Cog Systems D4 TOE to be Part 2 extended, and to meet the Security Assurance Requirements (SAR) contained in the MDFPP20.

10.1 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 HTC A9, Secured by Cog Systems D4 product 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.

10.2 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 MDFPP20 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.

10.3 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.

10.4 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.

10.5 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 MDFPP20 and recorded the results in a Test Report, summarized 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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database at the following URL: (https://web.nvd.nist.gov/view/vuln/search) and the Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "HTC A9, D4 Secure, msm8952, Android, Openssl, and Boringssl".

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.

10.7 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.

11 Validator Comments/Recommendations

The security functionality that was evaluated was scoped exclusively to the security functional requirements as specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the product, to include software or components that were not part of the evaluated configuration, need to be assessed separately and no further conclusions can be drawn about their effectiveness. For example, note that the ST specifies that: "The TOE includes the C2-Agent cell, the HSM Proxy cell, the Inner DAR cell and the Outer DIT cell that are not in the scope of this evaluation."

The validators encourage the consumers of these products to understand the relationship between the products and any functionality that may be provided via Mobile Device Management solutions. This evaluation neither covers, nor endorses, the use of any particular MDM solution; only the MDM interfaces of the products were exercised as part of the evaluation. In practice, the MDM application provided to perform functions as the administrator is not available, though its settings could be managed via a suitable MDM and corresponding agent. Alternatively, a downloadable application that can be utilized to put the

device into CC mode – "Android For Work", may also come pre-installed where required. The *HTC A9, Secured by Cog Systems D4 Administrator Guide Instructions* contains instructions on how the application can be acquired. As of the conclusion of this evaluation, an administrator can send an e-mail to md4support@cogsystems.com for the "testing app, guide, and the list of natively installed applications."

Consumers should note that the Android for Work application was used to place the device into the evaluated configuration; however, the application itself was not evaluated. The mobile devices must be configured into Common Criteria mode as directed in the *HTC A9, Secured by Cog Systems D4 Administrator Guide Instructions*, version 0.34, Sections 3.1 and 3.2, in order to be in the evaluated configuration.

Note that the evaluated configuration of the device does not support over the air (OTA) updates of its firmware, rather the device must be updated via the SD card. Note that while the device does have an SD card slot, it can be used only for provisioning the device. There is no access to the external SD card once the phone is booted up (e.g., from the Android OS the user has access to) therefore the use of SD card for any other functionality, such as data storage was neither tested nor evaluated.

In place of OTA updates, the Admin Guide informs users that bugs and vulnerabilities are addressed, along with patches applied, as they are reported. Customers are notified via e-mail when updates are available, including security updates for Android that are addressed in the monthly security bulletins. Once available, these updates can be downloaded "from the authorized Customer Portal." Users and enterprise administrators should remain cognizant of updates and the update cycles offered. The bug reporting process, along with contact information, can be found in Section 3.6 of the Admin Guide.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *HTC A9, Secured by Cog Systems D4 (MDFPP20) Security Target, Version 0.5, May 12, 2017*.

14 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.

15 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 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, 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 2102.

[4] Protection Profile For Mobile Device Fundamentals, Version 2.0, 17 September 2014

[5] HTC A9, Secured by Cog Systems D4 (MDFPP20) Security Target, Version 0.5, May 12, 2017 (ST)

[6] Assurance Activity Report (MDFPP20) for HTC A9, Secured by Cog Systems D4, Version 0.3, May 19, 2017 (AAR)

[7] Detailed Test Report (MDFPP20) for HTC A9, Secured by Cog Systems D4, Version 0.2, May 12, 2017 (DTR)

[8] Evaluation Technical Report for HTC A9, Secured by Cog Systems D4, Version 0.2, May 12, 2017 (ETR)

[9] HTC A9, Secured by Cog Systems D4 Adminstrator Guide Instructions, 6 March 2017, version 0.34