National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Cog Systems

Level 1, 277 King Street

Newton NSW 2042 Australia

D4 Secure VPN Client for the HTC A9 Secured by Cog Systems

Report Number: CCEVS-VR-10855-2017
Dated: November 16, 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
John Butterworth
Joanne Fitzpatrick
The MITRE Corporation

Ken 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 of the evaluation of D4 Secure VPN Client for the HTC A9 solution secured 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 November 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. 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 IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013.

The Target of Evaluation (TOE) is the D4 Secure VPN Client for the HTC A9 secured by Cog Systems.

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 D4 Secure VPN Client for the HTC A9 Secured by Cog Systems (IVPNCPP14) Security Target, version 0.7, October 31, 2017 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing

laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

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

- The 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	D4 Secure VPN Client for the HTC A9 secured by Cog Systems (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
ST	D4 Secure VPN Client for the HTC A9 secured by Cog Systems (IVPNCPP14) Security Target, version 0.7, October 31, 2017
Evaluation Technical Report	Evaluation Technical Report for Secure VPN Client for the HTC A9, version 0.3, November 15, 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
	John Butterworth, The MITRE Corporation
	Joanne Fitzpatrick, The MITRE Corporation
	Ken 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 (TOE) is the D4 Secure VPN Client that is the HTC A9 Secured by Cog Systems D4 Secure Mobile device's built-in Outer Data-In-Transit (DIT) VPN client. The Outer DIT VPN runs only on the evaluated HTC A9 Secured by Cog Systems D4 Secure Mobile device.

The D4 Secure is a smartphone based upon an HTC A9 hardware which uses Qualcomm SoCs (Snapdragon 617, MSM8952) and runs custom Cog Systems D4 Secure images. This is a custom built smartphone intended to support military and civil service users. The D4 Secure Mobile Device is the TOE Platform for the Outer DIT VPN client. Since the Outer DIT VPN is built-into the evaluated D4 Secure Mobile device, it is considered to have the same version as the D4 Secure Mobile device.

The TOE provides always on secure remote network connectivity for the D4 Secure and Android 6.0.1 operating system, by providing an IPsec VPN that once configured, protects all data communication. The Outer DIT VPN client sends all network communication to the connected VPN gateway through an IPsec protected communication channel.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the D4 Secure VPN Client for the HTC A9.

3.2 TOE Architecture

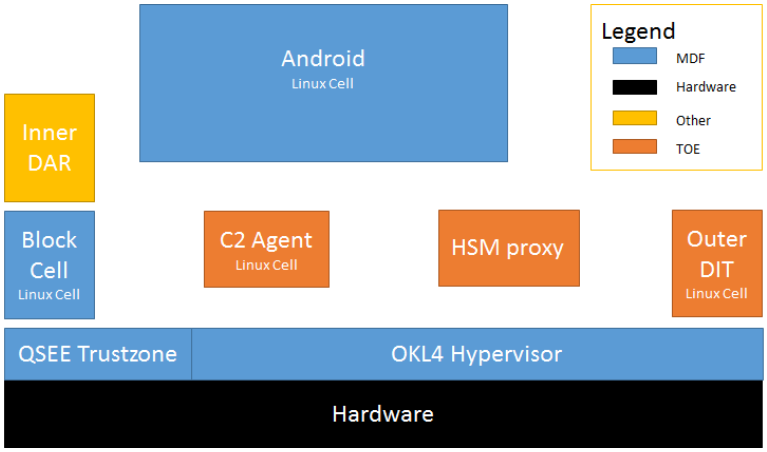
The TOE is a built-in VPN client (referred to as the Outer DIT). The cell providing the TOE's built-in VPN client is referred to as the Outer DIT cell. The TOE also includes a "C2 Agent" cell and an "HSM proxy" cell. These cells cooperate with the Outer DIT cell to facilitate interaction with the TOE Platform[1]. All IPSec protocol functions are provided by the TOE. All network traffic from the Android Cell is passed through the Outer DIT cell by the platform, thus ensuring that the Outer DIT VPN can protect all traffic.

The VPN Client relies upon its platform for the random numbers with which it seeds its own DRBG. All cryptography supporting the IPsec protocol stack is provided by the TOE. Data stored by the TOE utilize functions offered by the platform.

The following figure depicts the "Cells" in the D4 Secure Mobile Device. The figure shows the Outer DIT VPN client (i.e., Outer DIT cell, C2 Agent cell and HSM proxy cell), as well as the D4 Secure Mobile cells supporting the Outer DIT VPN Client. The D4 Secure Mobile Device is packaged to include all of the pieces shown in Figure 3-1. The "blue", "yellow" and "black" boxes in Figure 3-1 represent software that is part of the TOE Platform. The TOE is composed of only the cells shown in orange. The Outer DIT cell and C2 agent cell are running a Linux kernel that provides an environment for the cell's functionality. The HSM proxy cell is a cell running customized C language code.

[1] Refer to the Platform Security Target, VID 10776 for a description of platform cells.

Figure 3-1 D4 Secure Mobile Architecture



The TOE platform ensures that all network traffic from the Android cell passes through the Outer DIT cell which encapsulates the traffic in an IPsec tunnel. The outer DIT cell is a Linux 3.10.84 kernel with StrongSwan version 5.5.1 IPsec, OpenSSL 2.0.14 cryptographic library, and other non-cryptographic supporting libraries. The Outer DIT cell interacts with other cells (specifically the Android cell) via virtualized Ethernet. This ensures that the communication from the Android cell must pass through the Outer DIT cell (irrespective of whether the phone is connected via Wi-Fi or Mobile) and thus through the D4 Secure VPN Client.

The administrator configures the D4 Secure VPN client using a physically connected provisioning workstation. The provisioning workstation directly writes to the phone's internal, non-volatile memory after the user has unlocked the mobile device. The user cannot change the configuration once the device has been provisioned.

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 designed to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

The D4 Secure Outer DIT VPN Client runs entirely within the outer DIT cell of the D4 Secure mobile device. From a cryptographic perspective, all cryptography is performed using TOE software running in the Outer DIT VPN cell. The Outer DIT VPN cell (the TOE) relies upon the TOE platform for the random numbers with which the Outer DIT VPN cell seeds its own DRBG. All subsequent requirements for random values by Outer DIT VPN cell software obtain those values from the Outer DIT VPN cell's own DRBG. The Outer DIT VPN cell relies upon the TOE platform to verify the validity of updates.

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. Trusted path/channels

4.1 Cryptographic support

The IPsec implementation is the primary function of the TOE. IPsec is used by the TOE to protect communication between itself and a VPN Gateway over an unprotected network. The TOE also includes cryptographic services to support the IPsec VPN, and the self-testing functionality specified in this Security Target.

4.2 User data protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

4.3 Identification and authentication

The TOE provides the ability to use pre-shared keys and X.509 certificates that are used for IPsec Virtual Private Network (VPN) connections. The TOE utilizes TOE Platform functions to store and protect X.509 certificates.

4.4 Security management

The TOE provides the interfaces necessary to manage the security functions identified throughout this report to the administrator at provisioning. This includes interfaces to the VPN gateway. The IPsec VPN is fully configurable through a provisioning process that is performed prior to the first use of the D4 Secure Mobile Device. The TOE platform provides the functions necessary to securely update the TOE.

4.5 Protection of the TSF

The TOE utilizes its own cryptographic functions to perform self-tests that cover the TOE cryptographic operations. The TOE relies upon its underlying platform to perform self-tests that cover the TOE and the functions necessary to securely update the TOE.

4.6 Trusted path/channels

The TOE acts as a VPN client using IPsec to establish secure channels to corresponding VPN gateways.

5 Assumptions

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

- Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013

That information has not been reproduced here and the IVPNCPP14 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 IVPNCPP14 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 Protection Profile for IPsec Virtual Private Network (VPN) Clients 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 IVPNCPP14 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:

- D4 Secure VPN Client Guide Documentation, Version 1.1, October 31, 2017

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 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 Assurance Activity Report (IVPNCPP14) for D4 Secure VPN Client for the HTC A9, Version 0.3, November 15, 2017 (AAR).

8.1 Developer Testing

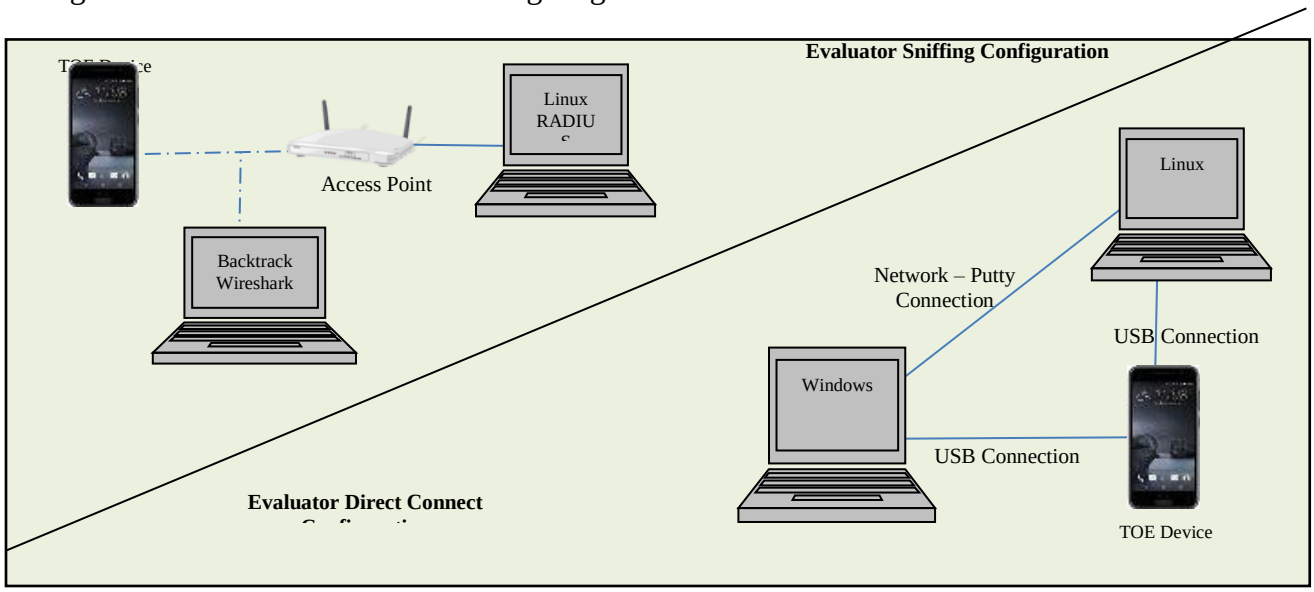
No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the IVPNCPP14 including the tests associated with optional requirements.

8.3 Test Configuration

The evaluation team exercised the independent tests specified in the *IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 (IVPNCPP14)* against the evaluated configuration of the TOE. The following diagram indicates the test environment.



Test Configuration

9 Evaluated Configuration

The evaluated configuration consists of the D4 Secure VPN Client for the HTC A9 on the evaluated platform, HTC A9, Secured by Cog Systems D4 mobile device.

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 D4 Secure VPN Client for the HTC A9 TOE to be Part 2 extended, and to meet the SARs contained in the IVPNCPP14.

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 D4 Secure VPN Client for the HTC A9 secured by Cog Systems products 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 IVPNCPP14 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 IVPNCPP14 and recorded the results in a Test Report, as summarized in the Assurance Activity Report.

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 (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "strongswan", "charon", "libcharon'libstrongswan", "libhydra".

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 product in its evaluated configuration relies upon a specific NIAP evaluated mobile device platform. That platform was evaluated under NIAP VID 10776.

The TOE security functionality that was evaluated was scoped exclusively to the security functional requirements as specified in the TOE Security Target, as instantiated upon the evaluated platform; the HTC A9, Secured by Cog Systems D4. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

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 and only the MDM interfaces of the products were exercised as part of the evaluation.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *D4 Secure VPN Client for the HTC A9 secured by Cog Systems (IVPNCPP14) Security Target, Version 0.7, October 31, 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 2012.

[4] Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013

[5] D4 Secure VPN Client for the HTC A9 secured by Cog Systems (IVPNCPP14) Security Target, Version 0.7, October 31, 2017 (ST)

[6] Assurance Activity Report (IVPNCPP14) for D4 Secure VPN Client for the HTC A9, Version 0.3, November 15, 2017 (AAR)

[7] Detailed Test Report (IVPNCPP14) for D4 Secure VPN Client for the HTC A9, Version 0.2, October 30, 2017 (DTR) <Evaluation Sensitive>

[8] Evaluation Technical Report for D4 Secure VPN Client for the HTC A9, Version 0.3, November 15, 2017 (ETR) <Evaluation Sensitive>

[9] D4 Secure VPN Client Guide Documentation, Version 1.1, October 31, 2017