National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Oceus Networks VPN Client (IVPNCPP14)

Report Number: CCEVS-VR-VID10754-2017
Dated: February 3, 2017
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

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Dr. Patrick Mallett
Lisa Mitchell
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
Raymond Smoley
Katie Sykes
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 TOE Evaluated Configuration 4
3.2 Physical Boundaries 4
4 Security Policy 4
4.1 Cryptographic support 5
4.2 User data protection 5
4.3 Identification and authentication 5
4.4 Security management 5
4.5 Protection of the TSF 5
4.6 Trusted path/channels 5
5 Assumptions 5
6 Clarification of Scope 6
7 Documentation 6
8 IT Product Testing 6
8.1 Developer Testing 7
8.2 Evaluation Team Independent Testing 7
9 Evaluated Configuration 8
10 Results of the Evaluation 8
10.1 Evaluation of the Security Target (ASE) 8
10.2 Evaluation of the Development (ADV) 8
10.3 Evaluation of the Guidance Documents (AGD) 9
10.4 Evaluation of the Life Cycle Support Activities (ALC) 9
10.5 Evaluation of the Test Documentation and the Test Activity (ATE) 9
10.6 Vulnerability Assessment Activity (VAN) 9
10.7 Summary of Evaluation Results 10
11 Validator Comments/Recommendations 10
12 Annexes 10
13 Security Target 10
14 Glossary 10
15 Bibliography 11

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation Team of the evaluation of Oceus Networks VPN Client (IVPNCPP14) solution provided by Oceus Networks, Inc. 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 January 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 Oceus Networks® VPN Client for Android Devices, Version 2.0.0.0.2211; and Oceus Networks® VPN Client for Samsung Devices, Version 2.0.0.0.2211.

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 evaluation results produced by the Evaluation Team. The Validation Team found that the evaluation showed that the product satisfies all 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 Oceus Networks VPN Client (IVPNCPP14) Security Target, Version 0.9, January 19, 2017 and analysis performed by the Validation Team.

The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:

- TD0031: ANSI X9.31 Reference in FCS_CKM.1(2) in VPN GW EP,

- TD0037: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4,
- TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1,
- TD0138: IPsec VPN Client Testing of SPD Rules,
- TD0140: FCS_IPSEC_EXT.1.12, Test 1 - Importing of Private Key and Certificate.

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:	Oceus Networks VPN Client, Version 2.0
Protection Profile	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
ST:	Oceus Networks VPN Client (IVPNCPP14) Security Target, Version 0.9, January 19, 2017
Evaluation Technical	Evaluation Technical Report for Oceus Networks VPN Client (IVPNCPP14),

Item	Identifier
Report	Version 0.3, January 19, 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	Oceus Networks, Inc.
Developer	Oceus Networks, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Paul Bicknell Dr. Patrick Mallett Lisa Mitchell The MITRE Corporation

3 Architectural Information

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

The TOE is a VPN client that provides secure remote network connectivity for Android 6.x mobile devices by implementing an IPsec VPN using the configurations defined by profiles. The IPsec VPN capabilities are 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 relies upon its platform for random numbers with which it seeds its own DRBG. All cryptography and the IPsec protocol stack are provided by the TOE.

Data stored by the TOE utilizes the evaluated platform's Data-at-rest protections provided by the TOE platform. However, the TOE implements its own protections for profiles which use PBKDF2WithHmacSHA1 (AES 256, CBC, PKCS 5 padding).

The TOE is a user space application that is installed as an APK. Internally it has 'application services' that run in the background and within the context of Java but do not run as a 'system service.' The TOE is released in two different APK (Application Packages) variations to better support Samsung KNOX and other non-KNOX Android platforms. The underlying VPN implementation is the same for both application packages. That is, the cryptographic libraries, VPN APIs and certificate management are the same in both application packages. The difference between the application packages is the APIs used to integrate with third party Mobile Device Management agents. On Samsung Devices, the TOE supports the KNOX MDM management APIs; while on the non-KNOX TOE version for Android, the TOE uses a proprietary SDK provided by Oceus Networks. The only difference in behavior is the handling of certificates when the revocation status of the certificate cannot be checked. On the non-KNOX version for Android, the TOE will always reject such certificates, while on Samsung Devices, the TOE will prompt the user for a decision on whether to accept the certificate.

The TOE employs a cross-platform implementation that utilizes a FIPS 140-2 level 1 certified cryptographic code base (Mocana NanoCrypto) providing IPsec/VPN encryption. The TOE is interoperable with current IKEv1 and IKEv2 RFCs and can utilize X509v3 certificates for authentication of an IPsec peer. In a basic IPsec VPN connection, all traffic from the VPN client is encrypted and sent across the VPN gateway. Profiles can be defined on or loaded into a mobile device. Named profiles define the endpoints, authentication data, and cryptographic characteristics for a VPN. Profiles define the cryptographic configuration of IKEv1 and IKEv2, tunnel mode, as well as a large set of additional cryptographic options.

3.1 TOE Evaluated Configuration

The Oceus Networks VPN Client runs on any Android 6.x platform. This includes the currently evaluated Samsung Galaxy mobile Android devices using these versions of Android (i.e., Galaxy S6, S6 Edge, Galaxy S7 and S7 Edge). The OVPN is installed on the mobile device and provides an interface to define and view profiles (a set of configuration values), as well as to establish and terminate VPN connections. The OVPN relies upon its platform for random numbers with which it seeds its own DRBG. All cryptography and the IPsec protocol stack are provided by the TOE. IPsec is used by the TOE to protect communication between itself and a VPN gateway over an unprotected network.

3.2 Physical Boundaries

The Oceus Networks VPN Client runs entirely within the context of the mobile device upon which it is installed. From a cryptographic perspective, all cryptography is performed using TOE software. The TOE relies upon the TOE platform for random numbers with which the TOE seeds its own DRBG. All subsequent need for random values by TOE software obtain those values from the TOE's own DRBG. The TOE also relies upon the platform to verify the validity of TOE updates.

4 Security Policy

This section summarizes 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 provides its cryptographic services to support the IPsec VPN, and 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, store, and protect X.509 certificates that are used for IPsec Virtual Private Network (VPN) connections.

4.4 Security management

The TOE provides all the interfaces necessary to manage the security functions identified throughout this Security Target. This includes interfaces to the user as well as to the VPN gateway. The IPsec VPN is fully configurable by a combination of functions provided directly by the TOE and those available to the associated VPN gateway. 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. The TOE platform provides 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 Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 (IVPNCPP14). That information has not been reproduced here and the IVPNCPP14 should be consulted if there is interest in that material.

6 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 Protection Profile for IPsec Virtual Private Network (VPN) Clients and performed by the Evaluation Team).
2. This evaluation covers only the specific product version identified in this document, and not any earlier or later versions released or in process.
3. 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.
4. 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 documentation was used as evidence for the evaluation of the Oceus Networks VPN Client:

- Oceus Networks VPN Client User Guide, Version 0.16, 12/8/2016
- Oceus Networks VPN Client Product Guidance, Version 0.8, 12/8/2016

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products 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 Detailed Test Report for Oceus Networks VPN Client (IVPNCPP14), Version 0.2, December 23, 2016, which is not publicly available. The *Assurance Activities Report (IVPNCPP14) for Oceus Networks VPN Client, Version 0.6, 01/19/17* (AAR), provides a non-proprietary overview of testing and the prescribed assurance activities.

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

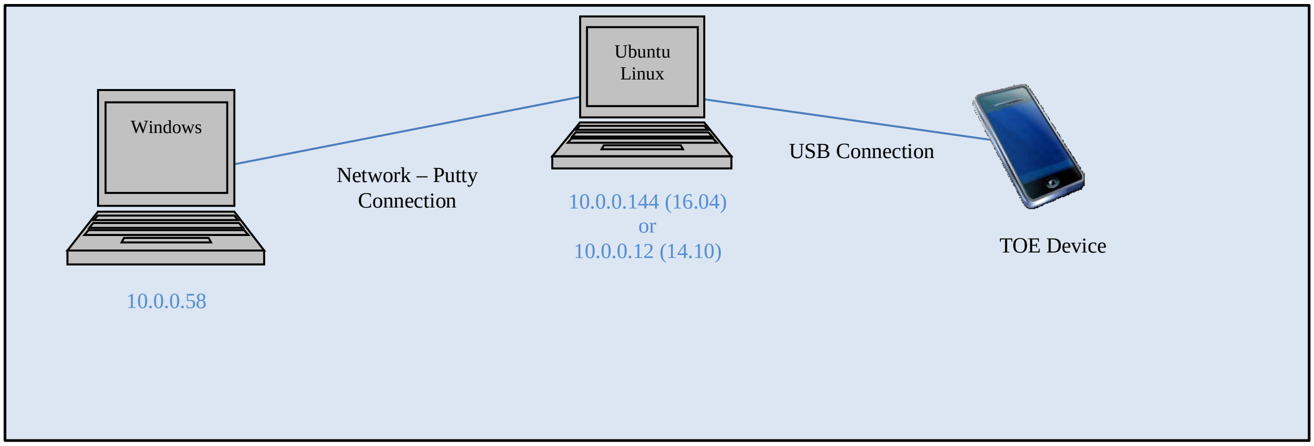

Figure 1 Evaluator Test Setup 1

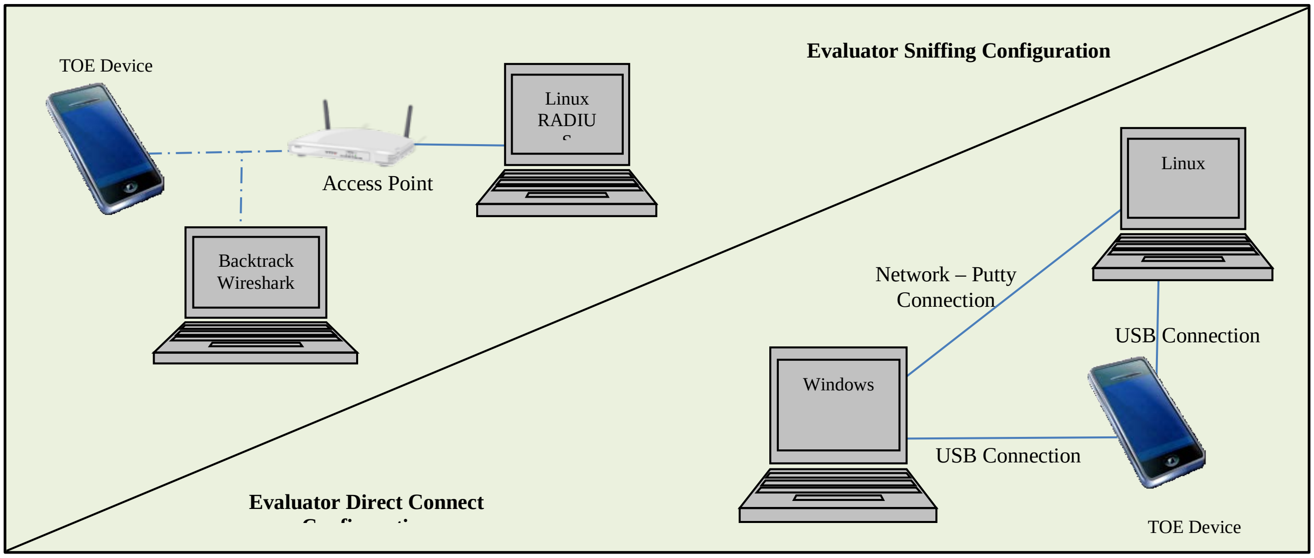

Figure 2 Evaluator Test Setup 2

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 the Oceus Networks VPN Client User Guide, Version 0.16, 12/8/2016 and the Oceus Networks VPN Client Product

Guidance, Version 0.8, 12/8/2016 documents and ran the tests specified in the IVPNCPP14. The Evaluation Team also performed a public search for vulnerabilities.

9 Evaluated Configuration

The evaluated configuration consists of the Oceus Networks VPN Client devices configured as specified in the Oceus Networks VPN Client User Guide, Version 0.16, 12/8/2016 and the Oceus Networks VPN Client Product Guidance, Version 0.8, 12/8/2016 documents.

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 Oceus Networks VPN Client 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 Oceus Networks VPN Client products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 (i.e., the TSS) 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 Validator reviewed the work of the Evaluation Team, and found that the conclusions reached by them were 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 the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

Additionally, the evaluator performed the assurance activities specified in the IVPNCPP14 related to the examination of the information contained in the guidance documents. The Validator reviewed the work of the Evaluation Team, and found that the conclusions reached by the Evaluation Team were 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.

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, summarized in the AAR.

Additionally, the evaluator performed the assurance activities specified in the IVPNCPP14 related to testing. The Validator reviewed the work of the Evaluation Team, and found that the conclusions reached by the Evaluation Team were 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: "Oceus Networks VPN Client", "ONVPNC", "Oceus Networks", "Oceus", "Mocana Nanosec", "Mocana".

The Validator reviewed the work of the Evaluation Team, and found 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 Validators suggest that the consumer pay attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements 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 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.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Oceus Networks VPN Client (IVPNCPP14) Security Target, Version 0.9, January 19, 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 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 IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013

[5] Oceus Networks VPN Client (IVPNCPP14) Security Target, Version 0.9, January 19, 2017 (ST)

[6] Assurance Activity Report (IVPNCPP14) for Oceus Networks VPN Client (IVPNCPP14), Version 0.6, 01/19/17 (AAR)

[7] Detailed Test Report (IVPNCPP14) for Oceus Networks VPN Client (IVPNCPP14), Version 0.3, January 19, 2017 (DTR)