National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Aruba, a Hewlett Packard Enterprise Company

3333 Scott Blvd

Santa Clara, CA 95054 USA

Aruba Virtual Intranet Access (VIA) Client Version 3.0

Report Number: CCEVS-VR-10871-2018
Dated: May 8, 2018
Version: 1.0

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

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

ACKNOWLEDGEMENTS

Validation Team

Meredith Hennan
Luke Florer
Kenneth Stutterheim,
The Aerospace Corporation

Common Criteria Testing Laboratory

Chris Keenan
Catherine Sykes
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 Aruba Virtual Intranet Access (VIA) Client Version solution provided by Aruba, a Hewlett Packard Enterprise Company. 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 2018. The information in this report is largely derived from the proprietary 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 Aruba Virtual Intranet Access (VIA) Client Version 3.0.

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 Aruba, a Hewlett Packard Enterprise Company Virtual Intranet Access (VIA) Client Version 3.0 (IVPNCPP14) Security Target, Version 1.5, May 3, 2018 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	Aruba Virtual Intranet Access (VIA) Client Version 3.0
Protection Profile	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
ST	Aruba, a Hewlett Packard Enterprise Company Virtual Intranet Access (VIA) Client Version 3.0 Security Target, Version 1.5, May 3, 2018
Evaluation Technical Report	Evaluation Technical Report for Aruba Virtual Intranet Access (VIA) Client Version 3.0, version 0.4, May 3, 2018
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	Aruba, a Hewlett Packard Enterprise Company
Developer	Aruba, a Hewlett Packard Enterprise Company
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Meredith Hennan, Luke Florer, Kenneth Stutterheim

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 Aruba, a Hewlett Packard Enterprise company Virtual Intranet Access (VIA) Client Version 3.0.

The Security Target focuses on the IPSEC VPN capabilities of the TOE. The TOE provides secure remote network connectivity for Linux, Android, and Windows mobile devices and workstations. The TOE has two primary purposes:

- to provide secure corporate access from employee workstations and smartphones
- to provide ease-of-use for the end users and network administrators

The IPsec VPN capabilities are the primary function of the TOE. IPSec is used by the TOE to protect communication between itself and an Aruba Mobility Controller over an unprotected network.

The TOE is a hybrid Internet Protocol Security (IPsec)/Secure Sockets Layer (SSL) VPN client available for multiple client operating systems. IPsec is the sole means of securing network traffic; SSL functionality involves encapsulation of IPsec inside HTTPS-formatted packets in order to traverse firewalls and proxies where required. SSL functionality is not included in this evaluation.

VIA can be downloaded directly from an Aruba Mobility Controller, pushed out using enterprise management tools, installed manually, or installed from the Google Play Store.

An Aruba Mobility Controller is required to terminate connections from a VIA client as VIA is not a general-purpose VPN client that will work with third-party VPN gateways.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

The TOE is the Aruba Virtual Intranet Access (VIA) client version 3.0 running on the following platforms:

- CC Evaluated on the following platforms running Android 7.1:
    - Samsung Galaxy S7
    - Samsung Galaxy S8
    - Samsung Note 8

The related Security Target for the Samsung evaluation can be found at https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10849

- CC Evaluated on the following versions of Windows Operating system:
    - Microsoft Windows 10 Home Edition (Anniversary Update, 32 and 64-bit versions)
    - Microsoft Windows 10 Pro Edition (Anniversary Update, 32 and 64-bit versions)

- Microsoft Windows 10 Enterprise Edition (Anniversary Update, 32 and 64-bit versions)
- Microsoft Windows Server 2016 Standard Edition
- Microsoft Windows Server 2016 Datacenter Edition
- TOE builds:
  - Windows 10, build 10.0.14393
  - Windows Server 2016, build 10.0.14393

The related Security Target for the evaluation can be found at https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2017.1007

- Linux (Red Hat Enterprise Linux 6.9 and CentOS Linux 6.9 with kernel version 2.6) – As the Linux platform was not evaluated, no Security Target exists.

  See:

  https://wiki.centos.org/Documentation

  or

  https://access.redhat.com/documentation/en-us/ red_hat_enterprise_linux/

  for associated documentation.

An Aruba Mobility Controller is required to be in the IT environment to communicate with the VIA Client. VIA is supported by an Aruba Mobility Controller running one of the following ArubaOS versions:

- ArubaOS 6.4
- ArubaOS 6.5
- ArubaOS 8.2

Note that some Aruba Mobility Controllers have been evaluated as part of NIAP; VID10569 and the associated Assurance Continuity Maintenance for ArubaOS versions 6.4 and 6.5x.

For this evaluation, product testing was performed using an Aruba Mobility Controller Model 7030 running ArubaOS 6.5.

An ArubaOS Advanced Cryptography (ACR) license must be installed on the Aruba Mobility Controller for the Suite B algorithms claimed in this ST to be available in the Aruba Common Cryptographic Module (CCM) version 1.0.0 and to enable client termination using these algorithms.

3.2 TOE Architecture

The VIA Client runs on an end-user device and communicates with a server component located on an Aruba Mobility Controller. The server component is used to manage the client and ensure policies are enforced. The Aruba Mobility controller maintains certain VIA configuration profiles, such as the VIA authentication profile, the VIA connection profile, and the VIA web authentication profile. Each profile plays an important role in authenticating the users and establishing a secure connection. When multiple authentication profiles are available, the VIA client prompts the user to select an authentication profile.

The first time a connection is established, a user opens the VIA client and enters the server name, username, and password. VIA then connects to the server over an HTTPS connection and attempts to authenticate using the user supplied credentials. If the VIA web authentication list has more than one VIA authentication profile, the user can choose a VIA authentication profile from the available ones. After successful authentication, the VIA client downloads the appropriate VIA connection profile and establishes the IPsec connection if the user is connected to an untrusted network.

At a protocol level, VIA operates over UDP port 4500, which is defined for IKE/IPsec traversal of NATs in RFC 3947. VIA uses HTTPS over TCP port 443 in order to contact the authentication server and download configuration profile updates before establishing each IKE/IPsec connection.

3.3 Physical Boundaries

The TOE is the Aruba Virtual Intranet Access (VIA) client version 3.0 running on the following platforms:

- Samsung Galaxy S7, Samsung Galaxy S8, Samsung Note 8 with Android 7.1 – CC evaluated. The Security Target for the evaluation can be found at https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10849
- Microsoft Windows 10 – CC evaluated. The Security Target for the evaluation can be found at https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2017.1007
- Linux (Red Hat Enterprise Linux 6.9 and CentOS Linux 6.9 with kernel version 2.6) – No CC evaluation exists for the platform, therefore there is no Security Target. See https://wiki.centos.org/Documentation or https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/ for associated documentation.

During evaluation testing, the VIA client 3.0 was tested using the following platforms:

- Samsung Galaxy S8 with Android 7.1
- Windows 10 Professional
- Centos 6.9

An Aruba Mobility Controller is required to be in the IT environment to communicate with the VIA Client. VIA Client 3.0 is supported by an Aruba Mobility Controller running one of the following ArubaOS versions:

- ArubaOS 6.4
- ArubaOS 6.5
- ArubaOS 8.2

An ArubaOS Advanced Cryptography (ACR) license must also be installed on the Aruba Mobility Controller for the Suite B algorithms claimed in this ST to be available and to enable client termination using these algorithms.

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 an Aruba Mobility Controller over an unprotected network.

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. In some cases, the storage and protection of X.509 certificates and keys is provided by the underlying operating system.

4.4 Security management

The TOE and its IPsec VPN are fully configurable by a combination of functions provided directly by the TOE and those available to the associated VPN gateway.

4.5 Protection of the TSF

The TOE performs self-tests that cover the TOE as well as the functions necessary to securely update the TOE.

4.6 Trusted path/channels

The TOE acts as a VPN client using IPsec to established 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 platform models and software as identified in section 3.1 of this document, and not any earlier or later versions released or in process of either the evaluated platforms hardware or software or client software.
- 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:

- Common Criteria Configuration Guidance, VPN Client Protection Profile, Aruba VIA Client v3.0, Version 2.0, March, 2018

To use the product in the evaluated configuration, the product must be configured as specified in that guide. Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device in its evaluated configuration. Consumers are encouraged to download this CC configuration guide from the NIAP website.

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 (IVPNCPP14) for Aruba Virtual Intranet Access (VIA) Client, Version 1.2, May 1, 2018 (DTR).

8.1 Developer Testing

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

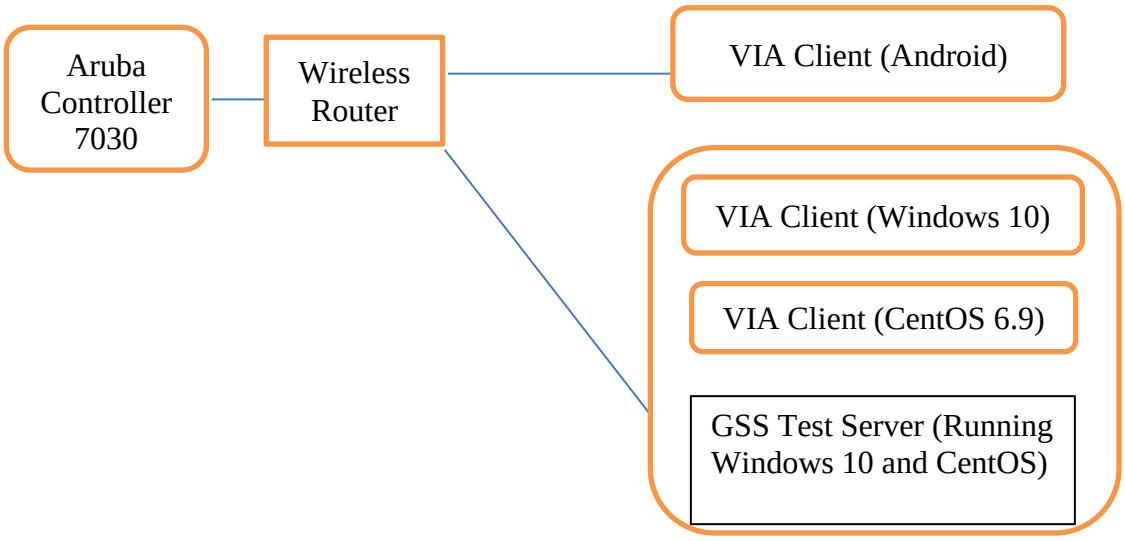
8.2 Evaluation Team Independent Testing

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 Tools

- Putty version 2013-11-27:r10097
- Wireshark version 1.12.5
- Microsoft Hyper-V (part of Windows)
- Standard Linux commands (e.g., cat, grep, awk)
- OpenSSL version 1.0.1f)
- tcpdump
- syslog-ng version 3.5.3-1
- stunnel4 version 4.53
- Evaluator developed test scripts to facilitate certificate test cases

8.4 Test Configuration



Additional detail on the evaluator's test environment and supporting products and tools can be found in Section 3.4 of the Assurance Activities Report (AAR).

9 Evaluated Configuration

The TOE is the Aruba Virtual Intranet Access (VIA) client version 3.0 running on the following platforms:

- Samsung Galaxy S7, Samsung Galaxy S8, Samsung Note 8 with Android 7.1 – CC evaluated. Security Target for the evaluation can be found at https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10849
- Microsoft Windows 10. - CC evaluated. Security Target for the evaluation can be found at https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2017.1007
- Linux (Red Hat Enterprise Linux 6.9 and CentOS Linux 6.9 with kernel version 2.6) – No CC evaluation or Security Target exists. See https://wiki.centos.org/Documentation or https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/ for associated documentation.

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, as characterized in the Assurance Activity Report for this evaluation, which is publicly available. 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 Aruba Virtual Intranet Access (VIA) Client Version 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 Aruba Virtual Intranet Access (VIA) Client Version 3.0 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 an evaluation sensitive Test Report, and summarized those results 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 (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/), Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities), Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories), Exploit / Vulnerability Search Engin (http://www.exploitsearch.net), SecurITeam Exploit Search (http://www.securiteam.com), Tenable Network Security (http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) on 2/27/2018, and again on 4/30/2018, with the following search terms: "aruba via", "virtual intranet access", "ipsec", "aruba mobility controller", "tls", "aruba vpn".

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

- VIA is not a general-purpose VPN client that works with third-party VPN gateways.
- An Aruba Mobility Controller is required to be in the IT environment to communicate with the VIA Client. The previously evaluated Aruba Mobility Controllers used ArubaOS 6.4 and 6.5. An Aruba Mobility Controller running Aruba OS 8.2 has not been evaluated as of the publication of this validation report, and as such, no claims to its secure operation nor proper operational integration with the client can be inferred from this evaluation.
- An ArubaOS Advanced Cryptography (ACR) license is required to be installed on the Aruba Mobility Controller for the Suite B algorithms claimed in this ST to be available and to enable client termination using these Suite-B algorithms or protocols. Operation of the device without the ACR module in the Mobility Controller places the device outside the evaluated configuration. Administrators will need to determine if the Aruba Mobility Controller in their Operational Environment requires the addition of the license to ensure the product is operated in the evaluated configuration.

- VIA supports both IKEv1 and IKEv2. However, only IKEv2 is to be used in the evaluated configuration.
- SSL functionality was not included in this evaluation. Administrators must ensure SSL is turned off in the Aruba Mobility Controller configuration.
- NIAP Labgram #72 interim guidance was exercised in the execution of this evaluation.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Aruba, a Hewlett Packard Enterprise Company Virtual Intranet Access (VIA) Client Version (IVPNCPP14) Security Target, Version 1.5, 05/03/2018*

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 IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013.

[5] Aruba, a Hewlett Packard Enterprise Company Virtual Intranet Access (VIA) Client Version (IVPNCPP14) Security Target, Version 1.5, 05/03/2018. (ST).

[6] Assurance Activity Report (IVPNCPP14) for Aruba Virtual Intranet Access (VIA) Client Version 3.0, Version 0.6, 05/03/2018 (AAR).

[7] Detailed Test Report (IVPNCPP14) for Aruba Virtual Intranet Access (VIA) Client Version 3.0, Version 1.2, May 1, 2018 (DTR). <Evaluation Sensitive>

[8] Evaluation Technical Report for Aruba Virtual Intranet Access (VIA) Client Version, Version 0.4, May 03, 2018 (ETR) <Evaluation Sensitive>

[9] Common Criteria Configuration Guidance, VPN Client Protection Profile, Target of Evaluation: Aruba VIA Client v3.0, Version 2.0, March 2018