National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

TM

SecuSUITE Client

Report Number:	**CCEVS-VR-VID10993-2020**
Dated:	**February 3, 2020**
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin: Senior Validator
Marybeth Panock: Lead Validator
Aerospace Corp

Common Criteria Testing Laboratory

Khai Van
Gossamer Security Solutions
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 BlackBerry SecuSUITE v4.0 solution. 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 2020. 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.

The Target of Evaluation (TOE) is the BlackBerry SecuSUITE v4.0.

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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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 SecuSUITE Client (ASPP13/PKGTLS11/VVoIPASEP10) Security Target, Version 0.7, January 30, 2020 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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) for Evaluation Assurance Level (EAL) 1 through 4 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:	BlackBerry SecuSUITE v4.0
	(Specific models identified in Section 3.1)
Protection Profile	Functional Package for Transport Layer Security (TLS), 1.1, March 2019
	Protection Profile for Application Software, Version 1.3, 1 March 2019[1]
	Application Software Protection Profile (App PP) Extended Package Voice/Video over IP (VVoIP) Endpoint, Version 1.0, 28 September 2016 (PKGTLS10/ASPP13/VVoIPASEP10)
ST:	SecuSUITE Client (ASPP13/PKGTLS11/VVoIPASEP10) Security Target, Version 0.7, January 30, 2020
Evaluation Technical Report	Evaluation Technical Report for BlackBerry SecuSUITE v4.0, Version 0.3, January 30, 2020.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	BlackBerry Limited
Developer	BlackBerry Limited
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	

3 Architectural Information

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

The Target of Evaluation (TOE) is BlackBerry SecuSUITE v4.0.

[1] Note: The NIAP page for the Functional Package, as well as the web version of the package, have a date of 2019-03-01. The PDF version of the package, which has the same version number, is dated 2019-02-12. For the purpose of this document, both dates are considered to be equivalent.

The TOE, herein referred to as the SecuSUITE Client or the TOE, is a VoIP application that executes on an Android or iOS mobile device operating system. The TOE executes on the following mobile devices:

a) Samsung Galaxy S9, S9+, S10, S10+, Note9, Note10 (Android 8.0/8.1)

b) Apple iPhone 8, 8 Plus, X, Xs, Xs Max, XR (iOS 12)

3.1 TOE Description

The TOE, herein referred to as the SecuSUITE Client or the TOE, is a VoIP application that executes on an evaluated mobile device operating system

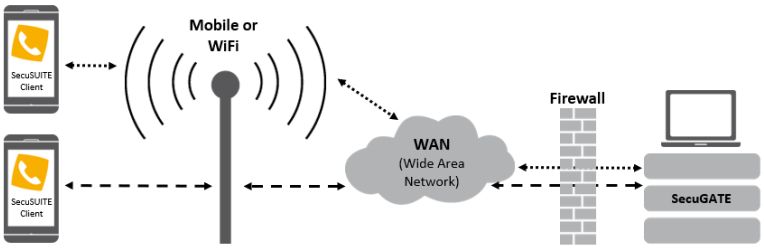

Figure 3-1 TOE Usage

User Context

The TOE user downloads the SecuSUITE Client from an app store (e.g. Apple Store, Google Play) or it is pushed via a Mobile Device Management (MDM) server (e.g. BlackBerry Enterprise Server) and installs the app to their mobile device. On first use of the app, the user must go through a registration process in order to register to a specified BlackBerry SecuGATE (identified by URI).

Once registered, the user can place secure VoIP calls using the app with largely the same interactions as with a normal phone call. The SecuSUITE Client provides encryption of user call signaling and voice data.

Users are typically invited to join SecuSUITE via an activation email initiated by their corporate IT administrator who adds users via the BlackBerry SecuGATE administration portal.

SecuSUITE Context

The TOE is part of the SecuSUITE Security Solution shown in Figure 3-2. The TOE does not work in isolation but relies on BlackBerry SecuGATE components to enable a secure VoIP communication.

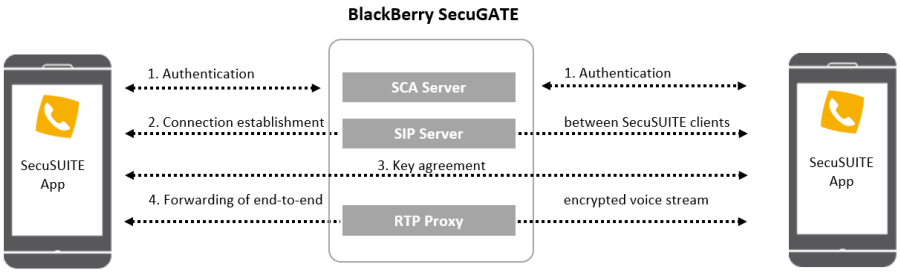

Figure 3-2 SecuSUITE Security Solution

As shown in Figure 3-2, the SecuSUITE VoIP process flow is as follows:

a) Step 1 Initial Registration. Every participating client has to register first to the Secure Client Authentication (SCA) server. The SCA server authenticates users and enrolls required client and user certificates as well as client configuration. Only clients that have been enrolled via the SCA service are able to connect to the SIP server and are allowed to establish end-to-end encrypted communication to other SecuSUITE clients. Note: Clients must also register to the SIP server using a SIP password. This is in addition to initial client registration with the SCA server.

b) Step 2 Connection establishment. The Session Initiation Protocol (SIP) together with TLS is used to establish a secure connection between mobile devices. The use of a TLS connection, providing encryption and mutual authentication, ensures that the devices connect with authorized SIP servers and the dialed call numbers are transmitted encrypted. The BlackBerry SecuGATE SIP Server Security Target defines the SIP Server TOE.

c) Step 3 Key agreement. When a call is placed and accepted, SecuSUITE clients exchange SIP messages that include digital certificates used to confirm caller identity and perform key agreement for SRTP encryption.

d) Step 4 End-to-end encrypted voice communication established. Clients utilize the SRTP protocol to exchange encrypted voice communications. The voice stream remains encrypted while traversing the BlackBerry SecuGATE and only the clients have access to the SRTP session keys.

e) Step 5 Forwarding of end-to-end encrypted voice stream. During connection signaling, the SIP server sets up the RTP/RTCP packet bridging in the Real-Time Transport Protocol (RTP) Proxy for this connection. The RTP Proxy relays / bridges the encrypted data stream between clients. The main purpose of the RTP Proxy is to make the communication between SIP user agents behind NAT/NAPT possible.

VoIP Client

The SecuSUITE Client establishes a secure tunnel for voice communications with another SecuSUITE client or the SecuGATE SIP server. The tunnel provides confidentiality, integrity, and data authentication for information that travels across the public network. This occurs using the Secure Real-Time Transport Protocol (SRTP) that has been established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDES) for SDP - the TOE supports SDES-SRTP.

The SecuSUITE Client also protects communications between itself and the SIP Server by using a Transport Layer Security (TLS)-protected signaling channel. To register the TOE within the domain, the TOE is required to be password authenticated by the SIP Server. The TOE also makes use of certificates to authenticate both the SIP server end and the TOE itself through the TLS connection.

Secure Text Messaging

The SecuSUITE client allows encrypted instant message transfer between client applications. Secure Text Messaging utilizes the same TLS protected SIP communication channel exactly the same way as other sensitive information (such as the SRTP encryption key) is transferred between the clients.

4 Security Policy

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

Note: *The ST should be consulted for more description of these and other security functions of the TOE.*

- Communication
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of the TSF
- TOE access
- Trusted path/channels

4.1 Communication

The TOE uses the SILK vocoder with a padding. The combination of the codec and padding ensures that the bit-rate is constant throughout the duration of the call

4.2 Cryptographic support

The TOE incorporates the OpenSSL cryptographic module to provide the cryptography in support of TLS and SRTP symmetric cryptography for bulk AES/AES-GCM encryption/decryption, SHA-2 algorithm for hashing, and HMAC for keyed hashing. In addition the TOE provides the cryptography to support EC-Diffie-Hellman key exchange and derivation function used in the TLS key establishment. The TOE platform provides ECDSA and RSA asymmetric cryptography for TLS peer authentication using digital signature and hashing services. In addition the TOE implements an SP 800-90A DRBG.

4.3 User data protection

The TOE secures media transmissions between itself and another VoIP endpoint. The TOE mediates the creation of SRTP channels between registered VoIP endpoints. The TOE enforces no additional information flow control policy rules, nor does it explicitly authorize or deny any information flows. The TOE protects sensitive data by storing secret and private keys using platform provided secure key storage, and it restricts access to platform provided resources.

4.4 Identification and authentication

The TOE and TOE platform perform device-level X.509 certificate-based authentication of the SIP server (ESC) during TLS. Device-level authentication allows the TOE to establish a secure channel with a trusted SIP server (ESC). The secure channel is established only after each endpoint successfully authenticates each other.

4.5 Security management

The TOE, TOE platform, and SIP server (ESC) provide the management functions to configure the security functionality provided by the TOE.

4.6 Privacy

The TOE does not collect any PII and does not intentionally transmit any PII over a network.

4.7 Protection of the TSF

The TOE performs a suite of self-tests during initial start-up to verify correct operation of its CAVP tested algorithms. Upon execution, the integrity of the TOEs software executables is also verified. The TOE Platform provides for verification of TOE software updates prior to installation.

4.8 TOE access

The TOE enforces a timeout on the SRTP channel. The timeout value is configurable on the SIP server (ESC).

4.9 Trusted path/channels

The TOE's implementation of TLS and SRTP provides a trusted channel ensuring sensitive data is protected from unauthorized disclosure or modification when transmitted from the host to a SIP server (ESC) and another VoIP endpoint, respectively.

5 Assumptions

The Security Problem Definition may be found in the ASPP13/PKGTLS11/VVoIPASEP10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The ASPP13/PKGTLS11/VVoIPASEP10 offers additional information about the identified security objectives, but that has not been reproduced here and the ASPP13/PKGTLS11/VVoIPASEP10 should be consulted if there is interest in that material.

In general, the ASPP13/PKGTLS11/VVoIPASEP10 has defined Security Objectives appropriate for software applications that provide Voice/Video over IP (VVoIP) endpoints and as such are applicable to the SecuSUITE Client TOE.

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 ASPP13/PKGTLS11/VVoIPASEP10 and performed by the evaluation team).
- This evaluation covers only the specific device models 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 ASPP13/PKGTLS11/VVoIPASEP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

The product provides the ability to interact with a PBX to route external calls, either to a external secure endpoint or a non-secure endpoint. These capabilities, called *Secure Landing* and *Breakout Calls*, are explicitly **excluded** from the evaluated configuration and were not covered by testing. Secure Landing and Breakout calls are covered under the SecuGATE ESC PP evaluation (VID 10977).

7 Documentation

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE (note that the first is Common Criteria specific and is normative while the others are generally informative) is as follows:

- Common Criteria Configuration Guide BlackBerry SecuSUITE 4.0, Version 1.3, 30-Jan-2020

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 (PKGTLS10/ASPP13/VVoIPASEP10) for SecuSUITE Client, Version 0.3, January 30, 2020(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 PKGTLS10/ASPP13/VVoIPASEP10 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration is SecuSUITE Client version 4.0.

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 5 and CEM version 3.1 rev 5. The evaluation determined the SecuSUITE Client version 4.0 TOE to be Part 2 extended, and to meet the SARs contained in the PKGTLS11, ASPP13 and VVoIPASEP10.

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 SecuSUITE v4.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 PKGTLS11, ASPP13 and VVoIPASEP10 related to the examination of the information contained in the TSS.

The validator 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 validator 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 validator 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 PKGTLS10, ASPP13 and VVoIPASEP10 and recorded the results in a Test Report, summarized in the AAR.

The validator 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 evaluator searched the National Vulnerability Database (NVD) from the NIST website to ensure no publicly known security flaws are identified for the TOE. The evaluator performed an initial search on November 27, 2019, with follow-up searches on January 3, 2020 and January 27, 2020. The following search terms were used:

- webrtc
- Boost
- ZLIB

- BZip2
- Openssl 1.0.2
- pjproject
- PocoCpp
- libphonenumber
- opus
- silk
- libsrtp
- secusmart
- secusuite

Android only terms:

- joda
- spongycastle
- androidannotations
- firebase
- androidx.appcompat
- zxing
- kotlin
- androidx.biometric

The public search for vulnerabilities did not uncover any residual vulnerability. The validator 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 validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Common Criteria Configuration Guide BlackBerry SecuSUITE 4.0, Version 1.3. No versions of the TOE and software, either earlier or later were evaluated.

Note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness. Specifically, as noted in the AGD, the SecuSUITE client differentiates between calls deemed secure (called "Secure Landing") and calls that are considered unprotected as they're routed potentially unencrypted to external numbers over untrusted networks (called "Breakout"). The ability of the SecuGATE SIP server to route calls to additional endpoints through a PBX lies beyond the scope of this ASPP13/PKGTLS11/VVoIPASEP10 evaluation and is not covered by the common criteria evaluation of the SecuSUITE client.

All other concerns and issues are adequately addressed in other parts of this document.

12 Annexes

Not applicable.

13 Security Target

The ST for this product's evaluation is SecuSUITE Client (PKGTLS10/ASPP13/VVoIPASEP10) Security Target, Version 0.7, 1/30/2020.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[5] SecuSUITE Client (PKGTLS10/ASPP13/VVoIPASEP10) Security Target, Version 0.7, 1/30/2020.

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

[7] Protection Profile for Application Software, Version 1.3, 1 March 2019

[8] Application Software Protection Profile (App PP) Extended Package Voice/Video over IP (VVoIP) Endpoint, Version 1.0, 28 September 2016

[9] Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019

[10] Evaluation Technical Report For SecuSUITE Client, 0.3, January 30, 2020

[11] Assurance Activity Report (PKGTLS10/ASPP13/VVoIPASEP10) for SecuSUITE Client, Version 0.3, January 30, 2020 (AAR)

[12] Detailed Test Report (PKGTLS11/ASPP13/VVoIPASEP10) for SecuSUITE Client, Version 0.3, January 29, 2020 (DTR)