National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

BlackBerry SecuSUITE Server Version 6.0

Report Number:	**CCEVS-VR-VID11634-2026**
Dated:	**January 27, 2026**
Version:	**1.0**

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Sheldon Durrant
Lisa Mitchell
Jaemond Reyes
Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Ryan Hagedorn
Khai Van

Gossamer Security Solutions, Inc.
Columbia, 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 Server Version 6.0 provided by BlackBerry Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) 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 Columbia, MD, United States of America, and was completed in January 2026. 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:

- *PP-Configuration for Network Device and Enterprise Session Controller (ESC)*, Version 2.0, 25 April 2024 (CFG_ND-ESC_V1.0)

  This PP-Configuration includes the following:

  - Base PP: *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e)
  - PP-Module: *PP-Module for Enterprise Session Controller (ESC)*, Version 1.0, 19 November 2020 (ESC10)
- *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10).

The TOE is the BlackBerry SecuSUITE Server Version 6.0. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 VR 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 (CCEVS) and the conclusions of the testing laboratory in the ETR 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 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *BlackBerry SecuSUITE Server Version 6.0 Security Target*, Version 0.7, January 23, 2026, 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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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 Server Version 6.0
Protection Profile	*PP-Configuration for Network Device and Enterprise Session Controller (ESC)*, Version 2.0, 25 April 2024 (CFG_ND-ESC_V1.0) This PP-Configuration includes the folllowing: • Base PP: *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e) • PP Module: *PP-Module for Enterprise Session Controller (ESC*), Version 1.0, 19 November 2020 (ESC10) *Functional Package for SSH,* Version 1.0, 13 May 2021 (SSH10)
ST	*BlackBerry SecuSUITE Server Version 6.0 Security Target*, Version 0.7, January 23, 2026
Evaluation Technical Report	*Evaluation Technical Report for BlackBerry SecuSUITE Server Version 6.0*, Version 0.3, January 23, 2026
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 Ltd.

Item	Identifier
Developer	BlackBerry Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Jaemond Reyes, Lori Sarem

3 Architectural Information

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

The SecuSUITE Server is the centerpiece in the SecuSUITE Security Solution. The SecuSUITE Security Solution includes the SecuSUITE Session Initiation Protocol (SIP) Server and client software[1] for mobile device platforms. Together these form a system that provides end-to-end secure mobile voice communication and instant messaging, using IP-based mobile data connections such as EDGE, UMTS/HSPA, LTE, and Wi-Fi.

The SecuSUITE Server is an infrastructure component of the SecuSUITE Security Solution. The SecuSUITE Server does not work in isolation but relies on other infrastructure components to enable secure VoIP communications.

3.1 TOE Description

The TOE is the SecuSUITE Server Version 6.0. The SecuSUITE Server enables use of SIP to establish secure connections between mobile devices.

3.2 TOE Evaluated Configuration

The SecuSUITE Server runs on RHEL 8 OS within an ESXi Version 8 virtualized environment using one of the following physical platforms:

- Dell PowerEdge R660 system with an Intel Xeon Silver 4510 processor (Sapphire Rapids microarchitecture) running ESXi 8
- PacStar 451 system with an Intel Xeon D-1539 (Broadwell microarchitecture) running ESXi 8.

The Dell PowerEdge R660 system can support either Broadcom Ethernet or Intel Ethernet network interfaces, while the PacStar 451 system supports only Intel Ethernet network interfaces.

3.3 TOE Architecture

The SecuSUITE SIP Server v6.0 is a network appliance providing SIP Server, RTP Proxy, and SCA functionality as well as interfaces for management. The SecuSUITE SIP Server TOE is composed of hardware, an internal supporting Red Hat Enterprise Linux OS (the TOE does not offer general purpose computer capabilities), and custom software. The custom software provides SIP Server, RTP Proxy, and SCA functionality. It runs on a Red Hat Enterprise Linux (RHEL 8) and utilizes the OpenSSL FIPS object module along with other supporting software.

Specifically, the TOE utilizes the Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module, which provides cryptographic functionality used by the TOE. The TOE's software executes on the RHEL 8 operating system on ESXi on a physical platform as specified in Section 3.2 above.

[1] The client software is the target for another evaluation.

3.4 Physical Boundaries

The TOE operates in a network environment mediating connections between VVoIP endpoints while utilizing services from other network entities.

SIP Server Functionality

The SIP Server interacts with the SecuSUITE VoIP client and provides registrar and proxy capabilities required for call-session management (e.g. establishing, processing, and terminating VoIP calls). As a SIP registrar, the SIP Server accepts REGISTER requests and places the information received into the location service on the SIP Server. As a SIP proxy server, the SIP Server is a stateful server that manages transactions to route SIP requests and responses. The SIP Server also provides a secure connection between mobile devices running the SecuSUITE app using TLS, providing encryption and mutual authentication.

RTP Proxy Functionality

The Real-Time Transport Protocol (RTP) Proxy bridges media packets sent between clients. The TOE creates and deletes RTP and Real-Time Transport Control Protocol (RTCP) bridging sessions in the RTP Proxy.

Secure Client Authentication Functionality (SCA0)

The SCA functionality authenticates users, facilitates VoIP client enrollment, and pushes client SIP configuration to the client. Only clients which have been enrolled via the SCA service are able to connect to the SIP Server. During SCA enrollment, the SCA authorizes authenticated clients (via activation code) to use the SIP Service and Additional Services and provisions them with the credentials and a TLS client certificate for the required trusted channels.

Additional Services functionality (SCA1)

SecuSUITE VoIP clients may interact with the TOE’s Additional Services using a dedicated mutually authenticated TLS trusted channel which is common for all Additional Services. Additional Services include e.g. Secure Contacts Push, Group Calling and Secure Text Messaging services. Information on the Additional Services can be found in the ST.

Attachment sharing

SecuSUITE clients may interact with the TOE to share larger content (e.g., media files) by using the TOE’s internal content sharing service. Connections between SecuSUITE clients and the TOE’s attachment sharing service are mutually authenticated TLS trusted channels.

NON-TOE Components

The TOE is part of a broader system (SecuSUITE security solution) and requires the following components to be present in the environment:

- Audit Server. The TOE is able to send audit logs to a remote syslog server.
- NTP Server. The TOE is able to obtain time from an NTP server using SHA256 as the message digest algorithm for authentication.
- Peer SIP Server. The TOE can communicate with another SIP server (such as Asterisk SIP or similar) over TLS.

- Push Server. The TOE can communicate with a push notification server that allows the VVoIP endpoint OS to execute deep sleep cycles and wake-up client applications for incoming events.
- VVoIP Endpoints. The TOE mediates connections initiated by a VVoIP client enrolled through the SCA Server to another VVoIP endpoint.
- S3 Gateway Server: The TOE may provide SeuSUITE clients with the ability to store their shared content to an external S3 Server.

4 Security Policy

This section summarizes the security functionality of the TOE:

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

4.1 Security audit

The TOE generates audit events for numerous activities including policy enforcement, system management, authentication, and system status (i.e., system log records). The TOE also generates call detail records providing information about connections that are mediated by the TOE. A syslog server in the environment is relied on to store audit and system log records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE appliance hardware.

4.2 Cryptographic support

The TOE contains CAVP-tested cryptographic implementations that provide key management, random bit generation, encryption/decryption, digital signature, and secure hashing and key-hashing features in support of higher-level cryptographic protocols, including HTTPS, NTP, SSH, and TLS.

4.3 User data protection

The TOE mediates connections between VVoIP endpoints, allowing enrolled endpoints to establish “calls” with other enrolled endpoints.

4.4 Identification and authentication

The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a username and password must be created for the user, and an administrative role must be assigned. The TOE performs the validation of the login credentials. The TOE also performs extensive X.509v3 certificate validation checks on certificates it receives as identification and authentication material.

4.5 Security management

The TOE also provides a Web UI (protected by HTTPS) and Command Line Interface (protected by SSH) to configure the TOE. Security management commands are limited to authorized users (i.e., administrators) and available only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled using privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Authorized Administrator role can manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management.

4.6 Protection of the TSF

The TOE implements features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability) and must obtain time from external time sources using NTP.

The TOE performs self-tests and integrity checks on TOE executables during system start-up as well as periodically during normal operation. The TOE also includes mechanisms (i.e., verification of the digital signature of each new update package) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.7 TOE access

The TOE can be configured to display a warning banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

4.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access, ensuring both integrity and disclosure protection. The TOE also provides a Web UI API interface for security management that is protected with HTTPS/TLS. If the negotiation of an encrypted session (either SSH or TLS) fails or if the user does not have authorization for remote administration, an attempted connection is not established.

The TOE protects communication with network peers, such as an audit server, VVoIP endpoints, ESC devices for trunking, S3 gateway server, and push notification server using TLS connections to prevent unintended disclosure or modification of data.

5 Assumptions & Clarification of Scope

5.1 Assumptions

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

- *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e)
- *PP-Module for Enterprise Session Controller (ESC),* Version 1.0, 19 November 2020 (ESC10)
- *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10)

That information has not been reproduced here and the NDcPP30e/ESC10/SSH10 should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP30e/ESC10/SSH10 as described for this TOE in the ST. 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.

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 NDcPP30e/ESC10/SSH10 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.
- Apart from the Admin Guide identified in Section 6, additional customer documentation for the specific TOE models was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.
- 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 NDcPP30e/ESC10/SSH10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following document was available with the TOE for evaluation:

- *BlackBerry SecuSUITE Server Common Criteria Configuration Guide SecuSUITE for Government 6.0*, Version 1.2, January 26, 2026

Any additional customer documentation provided with the product, or that is 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.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary *Detailed Test Report for BlackBerry SecuSUITE Server Version 6.0,* Version 0.3, January 23, 2026 (DTR), as summarized in the *Assurance Activity Report for BlackBerry SecuSUITE Server Version 6.0*, Version 0.3, January 23, 2026 (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the NDcPP30e/ESC10/SSH10. The AAR, in section 3.4.1 describes the tested devices, provides a list of test tools, and has diagrams of the test environment. The AAR is publicly available and not duplicated here.

8 Evaluated Configuration

The evaluated TOE models and evaluated configuration can be found in Section 3.2 of this report.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all 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 team determined the SecuSUITE Server Version 6.0 to be Part 2 extended, and to meet the SARs contained in the NDcPP30e/ESC10/SSH10.

9.1 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 BlackBerry SecuSUITE Server Version 6.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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.

9.2 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 ST and Guidance document. Additionally, the Evaluator performed the assurance activities specified in the NDcPP30e/ESC10/SSH10 related to the examination of the information contained in the TSS.

The Validation team 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.

9.3 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 NDcPP30e/ESC10/SSH10 related to the examination of the information contained in the operational guidance documents.

The Validation team 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.

9.4 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 Validation team 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.

9.5 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 NDcPP30e/ESC10/SSH10 and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the NDcPP30e/ESC10/SSH10, and that the conclusion reached by the Evaluation team was justified.

9.6 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 Evaluation team. The vulnerability analysis includes a public search for vulnerabilities.

The Evaluation team searched the following public vulnerability databases:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- MITRE CVE Database, National Vulnerability Database, and CVE details (https://www.cve.org/, https://web.nvd.nist.gov/vuln/search, and https://www.cvedetails.com/vulnerability-search.php)
- Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
- 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)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The Evaluation team performed vulnerability searches using the following key words. The search was performed on January 19, 2026:

"SecuGATE", "SecuSMART", "SecuSUITE", "VOIP", "stunnel", "SIP", "openssl", "ssh", "ntp", "tls", "ESXI", “Intel Xeon Silver 4510”, “Intel Xeon E-D-1539”, “RHEL 8”, and “RTP”.

The Evaluation team conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

The Validation team 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.

9.7 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 test activities 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, performed the Assurance Activities in the NDcPP30e/ESC10/SSH10 and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Guidance document defined in Section 6. No other versions of the TOE and software, either earlier or later, were evaluated.

The evaluated functionality is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionalities provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *BlackBerry SecuSUITE Server Version 6.0 Security Target, Version 0.7, January 23, 2026*.

13 **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.

14 **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 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, 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] *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e).

[5] *PP-Module for Enterprise Session Controller (ESC)*, Version 1.0, 19 November 2020 (ESC10).

[6] *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10).

[7] *BlackBerry SecuSUITE Server Version 6.0 Security Target*, Version 0.7, January 23, 2026 (ST).

[8] *Assurance Activity Report for BlackBerry SecuSUITE Server Version 6.0*, Version 0.3, January 23, 2026 (AAR).

[9] *Detailed Test Report for BlackBerry SecuSUITE Server Version 6.0*, Version 0.3, January 23, 2026 (DTR).

[10] *Evaluation Technical Report for BlackBerry SecuSUITE Server Version 6.0*, Version 0.3, January 23, 2026 (ETR).

[11] *BlackBerry SecuSUITE Server Common Criteria Configuration Guide SecuSUITE for Government 6.0*, Version 1.2, January 26, 2026 (AGD)