National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

SecuGATE Version 4.0

Report Number: **CCEVS-VR-VID10977-2019**
Dated: **December 19, 2019**
Version: **0.1**

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

Sheldon Durrant
Randy Heimann
Lisa Mitchell
Linda Morrison
Claire Olin
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Cornelius Haley
Khai Van
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 BlackBerry, SecuGATE SIP Server version 4.0. 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 December 2019. 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 collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21).

The Target of Evaluation (TOE) is the SecuGATE SIP Server version 4.0.

The 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 SecuGATE Version 4.0 (NDcPP21) Security Target, Version 0.7, December 19, 2019 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 Product Compliant 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, SecuGATE SIP Server version 4.0
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
ST	SecuGATE Version 4.0 (NDcPP21) Security Target, Version 0.7, December 19, 2019
Evaluation Technical Report	Evaluation Technical Report (NDcPP21) for SecuGATE SIP Server, Version 0.4, December 19, 2019
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
Developer	BlackBerry
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 SecuGATE SIP Server v4.0. The SecuGATE SIP Server TOE is composed of hardware, a hardened 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 7.6) and utilizes the OpenSSL FIPS object module along with other supporting software.

Specifically, the TOE utilizes the OpenSSL 1.0.2 FIPS object module v2.0.16 which provides cryptographic functionality used by the TOE. The TOE's software executes on the RHEL 7.6 operating system on ESXi on a physical platform that is the SUPERMICRO SuperServer with an Intel Xeon E3-1240, Xeon E3-1515, or Intel Xeon Gold 5218.

3.1 TOE Description

The TOE is the SecuGATE SIP server version 4.0. The SecuGATE SIP Server enables use of the Session Initiation Protocol (SIP) to establish secure connections between mobile devices.

The SecuGATE SIP Server is the centerpiece in the SecuSUITE Security Solution. The SecuSUITE Security Solution includes the SecuGATE SIP server and client software1 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 SecuGATE SIP Server v4.0 is network appliance providing SIP server, RTP Proxy and SCA functionality as well as interfaces for management.

3.2 TOE Evaluated Configuration

The Target of Evaluation (TOE) is SecuGATE SIP Server v4.0. The SecuGATE SIP Server v4.0 enables use of the Session Initiation Protocol (SIP) to establish secure connections between mobile devices. The SecuGATE SIP server runs on RHEL 7.6 OS within an ESXi version 6.5 virtualized environment using a physical platform which includes an Intel Xeon E3-1240, Xeon E3-1515 or Xeon Gold 5218 processor including:

- the SUPERMICRO system with an Intel Xeon E3-1240,
- the SUPERMICRO system with an Intel Xeon Gold 5218. and
- the PacStar 451 system with an Intel Xeon E3-1515.

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

3.3 Physical Scope of the TOE

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

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 SIP service and provisions them with the SIP credentials and a TLS client certificate for the required trusted channel.

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:

a) Audit server. The TOE is able to send audit logs to a remote syslog server.

b) NTP Server. The TOE is able to obtain time from an NTP server over a TLS protected session.

c) Peer SIP server. The TOE can communicate with another SIP server (such as Asterisk SIP or similar) over TLS.

d) 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.

e) VVoIP Endpoints. The TOE mediates connections initiated by a VVoIP client enrolled through the SCA Server to another VVoIP endpoint.

4 Security Policy

This section summaries 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 user name 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 through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Authorized Administrator role can actually 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 a number of features design 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 can 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 image) 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 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 be established.

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

5 Assumptions

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

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21)

That information has not been reproduced here and the NDcPP21 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 NDcPP21 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 NDcPP21 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 NDcPP21 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:

- SecuGATE Common Criteria Configuration Guide, SecuSUITE for Government 4.0, doc version 1.3

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 (NDcPP21) for SecuGATE SIP Server, Version 0.4, December 19, 2019(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 NDcPP21 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration is SecuGATE SIP Server 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 SecuGATE SIP Server version 4.0 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP21.

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 SecuGATE SIP Server version 4.0 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 NDcPP21 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 NDcPP21 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 this search on December 5, 2019. The following search terms were used:

- Secusmart
- Secugate
- RHEL
- TLS
- SSH
- SIP
- VOIP
- OpenSSL
- ntp
- tcp

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 SecuGATE Common Criteria Configuration Guide, SecuSUITE for Government 4.0, doc version 1.3. No versions of the TOE and software, either earlier or later were evaluated.

Please 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.

12 Annexes

Not applicable

13 **Security Target**

The Security Target is identified as*:* SecuGATE Version 4.0 (NDcPP21) Security Target, Version 0.7, December 19, 2019.

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 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 2.1, 24 September 2018 (NDcPP21).

[5] SecuGATE Version 4.0 (NDcPP21) Security Target, Version 0.7, December 19, 2019 (ST).

[6] Assurance Activity Report (NDcPP21) for SecuGATE SIP Server, Version 0.4, December 19, 2019 (AAR).

[7] Detailed Test Report (NDcPP21) for SecuGATE SIP Server, Version 0.4, December 19, 2019 (DTR).

[8] Evaluation Technical Report (NDcPP21) for SecuGATE SIP Server, Version 0.4, December 19, 2019 (ETR)

[9] SecuGATE Common Criteria Configuration Guide, SecuSUITE for Government 4.0, doc version 1.3 (CC-Guide)