Certification Report

EAL 2+ Evaluation of

Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS), Release v09.00

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-221-CR
Version: 1.0
Date: 14 September 2012
Pagination: i to iii, 1 to 12

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 14 September 2012, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademark or registered trademark:

- Sonus is a registered trademark of Sonus Networks, Inc.

TABLE OF CONTENTS

Executive Summary

Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS), Release v09.00 (hereafter referred to as Trunking Suite), from Sonus Networks, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Trunking Suite, a telephony trunking suite, is a distributed software Target of Evaluation (TOE) providing full integration between a packet infrastructure and a Public Switched Telephone Network (PSTN). Trunking Suite provides management functions through the Insight Element Management System (EMS) and provides all of the capabilities required to provide telephony service on a packet backbone for voice, data, and fax transmission.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 25 July 2012 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Trunking Suite, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentations are claimed: ALC_FLR.2 – Flaw reporting procedures and ALC_DVS.1 – Identification of security measures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Trunking Suite evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS), Release v09.00 (hereafter referred to as Trunking Suite), from Sonus Networks, Inc..

2 TOE Description

Trunking Suite, a telephony trunking suite, is a distributed software TOE providing full integration between a packet infrastructure and a Public Switched Telephone Network (PSTN).Trunking Suite provides management functions through the Insight Element Management System (EMS) and provides all of the capabilities required to provide telephony service on a packet backbone for voice, data, and fax transmission. The Policy and Router Server (PSX) is responsible for the main call processing functions in a packet network, including call screening and blocking, support for number translation services such as local number portability, calling name delivery, and toll-free services, call routing, and billing. DataStream Integrator Call Data Record Translation Engine ("DSI") is an advanced data translation engine that is used to collect, correlate, and produce a standards compliant billing stream according to customer-specific services and billing usage criteria.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Trunking Suite is identified in Section 6 of the ST.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Trunking Suite:

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS-PUB 197	2117
Rivest Shamir Adleman (RSA)	PKCS #1, v1.5	1098
Secure Hash Algorithm (SHA-1)	FIPS 180-4	1841
Hash-based message authentication code (HMAC) Secure Hash Algorithm (SHA-1)	FIPS 198-1	1289

4 Security Target.

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS), Release v09.00
Version: 1.0
Date: 20 July 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

Trunking Suite is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 2* augmented, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw reporting procedures and ALC_DVS.1 – Identification of security measures.

6 Security Policy

Trunking Suite implements three information flow policies:

- PEERED information flow control policy for the transfer of IP traffic and multimedia packets across the TOE from connected IT entities for onward transmission to other connected IT entities.

- AUTHENTICATED information flow control policy for EMS-initiated traffic to TOE subsystems for operational administration. This policy also enforces local operational and administrative CLI commands at each of the TOE subsystems.

- ENCRYPTED information flow control policy for intra-TOE channel security for operating and administering TOE subsystems via the EMS management interfaces over Hypertext Transfer Protocol (HTTPS), Transport Layer Security (TLS), and Secure Shell (SSH). This policy also enforces channel security for secure signalling for the GSX subsystem with peered telecommunications service providers by transporting signalling protocols over either TLS or IPSec.

In addition, Trunking Suite implements other policies pertaining to security audit, user data protection, cryptographic support, identification and authentication, security management, access to the TOE, trusted channel, protection of the TSF, and resource utilization. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Trunking Suite should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Administrators are non-hostile and follow all administrator guidance when using the TOE. Administration is competent and ongoing and administrators have the required rights necessary to manage the TOE; and
- Primary TOE Administrators manage roles that grant or revoke user's access within the Telecommunications Service Providers organization.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the operational environment;
- The TOE will be connected to the Telecommunication Service provider's core network, and external authentication services will be available and a Network Time Protocol (NTP) server be available;
- The TOE is connected to the Public Switched Telephone Network (PSTN) and Signaling System No. 7 (SS7) networks via Telecommunication Service Provider peering relationships; and
- There are no general purpose computing capabilities on the TOE other than those necessary for the correct operation, administration and support of the TOE.

7.3 Clarification of Scope

Trunking Suite offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. Trunking Suite is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

Trunking Suite incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

The evaluated configuration for Trunking Suite comprises:

Application / Network Element	**Software Version**
• Insight Element Management System (EMS)	Release V09.00.00A201
• GSX/NBS 9000 High-density Media Gateway Open Services Switch (GSX)	Release V09.00.00A203
• DataStream Integrator Call Data Record Translation Engine (DSI)	Release V09.00.00A201
• Policy and Routing Server (PSX)	Release V09.00.00A200
• SGX4000 SS7 Signaling Gateway (SGX)	Release V07.03.06R008

The publication entitled Common Criteria Evaluated configuration for Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS) release V09.00, Document No. 1744-000-D012, Version: 0.2, 24 July 2012 describes the procedures necessary to install and operate Trunking Suite in its evaluated configuration.

9 Documentation

The Sonus Networks, Inc. documents provided to the consumer are as follows:

- DataStream Integrator DSI Administration and Maintenance Guide (Solaris & Linux), Sonus Part Number: 550-05398, Document Version: 1, Software Version: V08.04.01;
- DSI DataStream Integrator Alarm Troubleshooting Guide, Sonus Part Number: 550-05399, Document Version: 1, Software Version: V08.04.01;
- DataStream Integrator Installation and Upgrade Guide (Linux), Sonus Part Number: 550-05397, Document Version: 1, Software Version: V08.04.01;
- DataStream Integrator DSI Installation and Upgrade Guide (Solaris), Sonus Part Number: 550-05396, Document Version: 1, Software Version: V08.04.01;
- DataStream Integrator DSI Installation and Upgrade Guide (Solaris), Sonus Part Number: 550-05396, Document Version: 1, Software Version: V08.04.01;
- DataStream Integrator (Linux) Version 8.4.1 Patch 1 Release Notes, Software Version: DSI 08.04.01R000, Document Number: 550-05534, Document Version: 1;
- Insight Element Management System Alarm Troubleshooting Guide, Sonus Part Number: 550-05404 Document Version: 1 Software Version: V08.04.01;
- Insight Element Management System Software Installation and Upgrade, Guide Sonus Part Number: 550-05413, Document Version: 1, Software Version: V08.04.01;
- Insight Version 08.04.01 Release Notes, Software Version: EMS

08.04.01R000, Document Number: 550-05414, Document Version: 2;

- Insight Element Management System Traffic Manager User Guide, Sonus Part Number: 550-05411, Document Version: 1, Software Version: V08.04.01;
- Insight Element Management System User Guide, Sonus Part Number: 550-05403, Document Version: 1, Software Version: V08.04.01;
- GSX9000 and GSX4000 Series Open Services Switch Alarm Troubleshooting Guide, Sonus Part Number: 550-05376 Document Version: 2 Software Version: V08.04.01;
- GSX9000 Open Services Switch Installation and Upgrade Guide, Sonus Part Number: 550-05374, Document Version: 1, Software Version: V08.04.01;
- GSX9000 and GSX4000 Series Open Services Switch Operations Guide, Sonus Part Number: 550-05375, Document Version: 1 Software Version: V08.04.01;
- GSX9000™ and GSX4000™ Open Services Switch Version 08.04.01F001 Release Notes, Software Version: GSX 08.04.01F001,Document Number: 550-05530, Document Version: 1;
- PSX Policy Server Alarm Troubleshooting Guide Sonus, Part Number: 550-05392, Document Version: 1, Software Version: V08.04.01;
- Sonus Insight CLI User Guide For PSX, Sonus Part Number: 550-05405, Document Version: 1, Software Version: V08.04.01;
- Sonus Insight CLI User Guide For PSX, Part Number 550-05405, Document Version 1, Software Version V08.04.01;
- PSX Policy Server Installation and Upgrade Guide, Sonus Part Number: 550-05389, Document Version: 1, Software Version: V08.04.01;
- PSX Policy Server Product Description Guide, Sonus Part Number: 550-05390, Document Version: 1, Software Version: V08.04.01;
- PSX Policy Server Provisioning Guide, Sonus Part Number: 550-05391, Document Version: 1, Software Version: V08.04.01;
- PSX Policy Server Version 08.04.01F001 Release Notes, Software Version: PSX 08.04.01F001, Document Number: 550-05582, Document Version: 1;
- Sonus Policy Server Tools Guide, Sonus Part Number: 550-05393 Document Version: 1 Software Version: V08.04.01;
- SGX4000 Signaling Gateway Alarm Troubleshooting Guide, Sonus Part Number: 550-05208, Document Version: 1, Software Version: V07.03.06;
- SGX4000 SS7 Gateway CLI User Guide, Sonus Part Number: 550-05207, Document Version: 1.0, Software Version: V07.03.06;
- SGX4000 Software Installation Guide, Sonus Part Number: 550-05269, Document: 1, Software: V07.03.06;
- SGX4000 SS7 Gateway Operations Guide, Sonus Part Number: 550-

05206, Document Version: 1, Software Version: V07.03.06;
- SGX4000 SS7 Gateway Version 7.3.6 Release Notes, Software Version: SGX4000 07.03.06R000, Document Number: 550-02656, Document Version: 2.0, February 28, 2011;
- Cross-Platform Alarm Troubleshooting Guide (Agent Framework Host Monitoring Linux Platform Monitoring RAID Sun Netra Agent System Management Veritas Management), Sonus Part Number: 550-05412, Document Version: 1, Software Version: V08.04.01; and
- Common Criteria Evaluated configuration for Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS) release V09.00, Document No. 1744-000-D012, Version: 0.2, 24 July 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Trunking Suite, including the following areas:

Development: The evaluators analyzed the Trunking Suite functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Trunking Suite security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Trunking Suite preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Trunking Suite configuration management system and associated documentation was performed. The evaluators found that the Trunking Suite configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Trunking Suite during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Sonus Networks, Inc. for Trunking Suite. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to

track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

The evaluators reviewed the development security documentation and policies as set forth by Sonus Networks, Inc. During a site visit to the developers' headquarters, the evaluators reviewed the development security measures in place. The evaluators concluded that the procedures and processes are sufficient and are being adhered to.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Trunking Suite. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Trunking Suite potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to Trunking Suite in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of EWA-Canada test goals:

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Independent Evaluator testing: The objective of this test goal is to exercise the TOE's claimed functionality through evaluator independent testing: Tests covered in this area include:

- Initialization: The objective of this test goal is to provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

- Identification and authentication:

  Verify that the TSF shall detect the unsuccessful authentication attempts made by a user as configured by an administrator and lock the user account.

  Verify that TSF maintains security attributes of users.

  Verify that users are successfully authenticated before allowing TSF mediated actions.

- Security Management:

  Verify that administrator user can perform remote monitoring using CLI.

  Verify that GSX subsystem operator cannot configure the IP input filter.

  Verify that users can only perform actions accorded to their role.

- Resource Utilization:

  Verify that TSF assigns a priority to High Probability of Completion (HPC) call during times of network stress and or congestion.

  Verify that an alarm is raised on reaching an established threshold on GSX subsystem.

- User Data Protection:

  Verify that communication between parts of the TOE is happening over a secure channel.

- Security Audit:

  Verify that TSF records the start-up and shutdown of the audit functions

Verify that administrators have the capability to read audit records.

Verify that audit records are provided in a manner suitable for proper interpretation.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- EMS Node Locking (tampering): The purpose of this test is to verify that concurrent administrators cannot tamper with a network element if locked by another administrator.

- Direct Attack: The purpose of this test case is to verify that an attacker cannot circumvent the main login for Insight Element Management System.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

Trunking Suite was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Sonus site in Westford, MA. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Trunking Suite behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 2 + level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The complete documentation for the Trunking Suite includes comprehensive Installation and Users Guides. The developer has extensive process documentation to support the development of the product.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
DSI	Datastream Integrator Call Data Record Translation Engine
EAL	Evaluation Assurance Level
EMS	Insight Element Management System
ETR	Evaluation Technical Report
HMAC	Hash-based Message Authentication Code
HPC	High Probability of Completion
HTTPS	Hypertext Transfer Protocol
IPSec	Internet Protocol Security
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
PSTN	Public Switched Telephone Network
PSX	Policy and Router Server
RSA	Rivest Shamir Aldeman
SFR	Security Functional Requirements
SHA-1	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS), Release v09.00, version 1.0, 20 July 2012 Security Target.

e. Sonus Trunking Suite(GSX/NBS 9000,SGX 4000,PSX,DSI,EMS), Release 09.00, version 1.2, July 25, 2012 ETR.