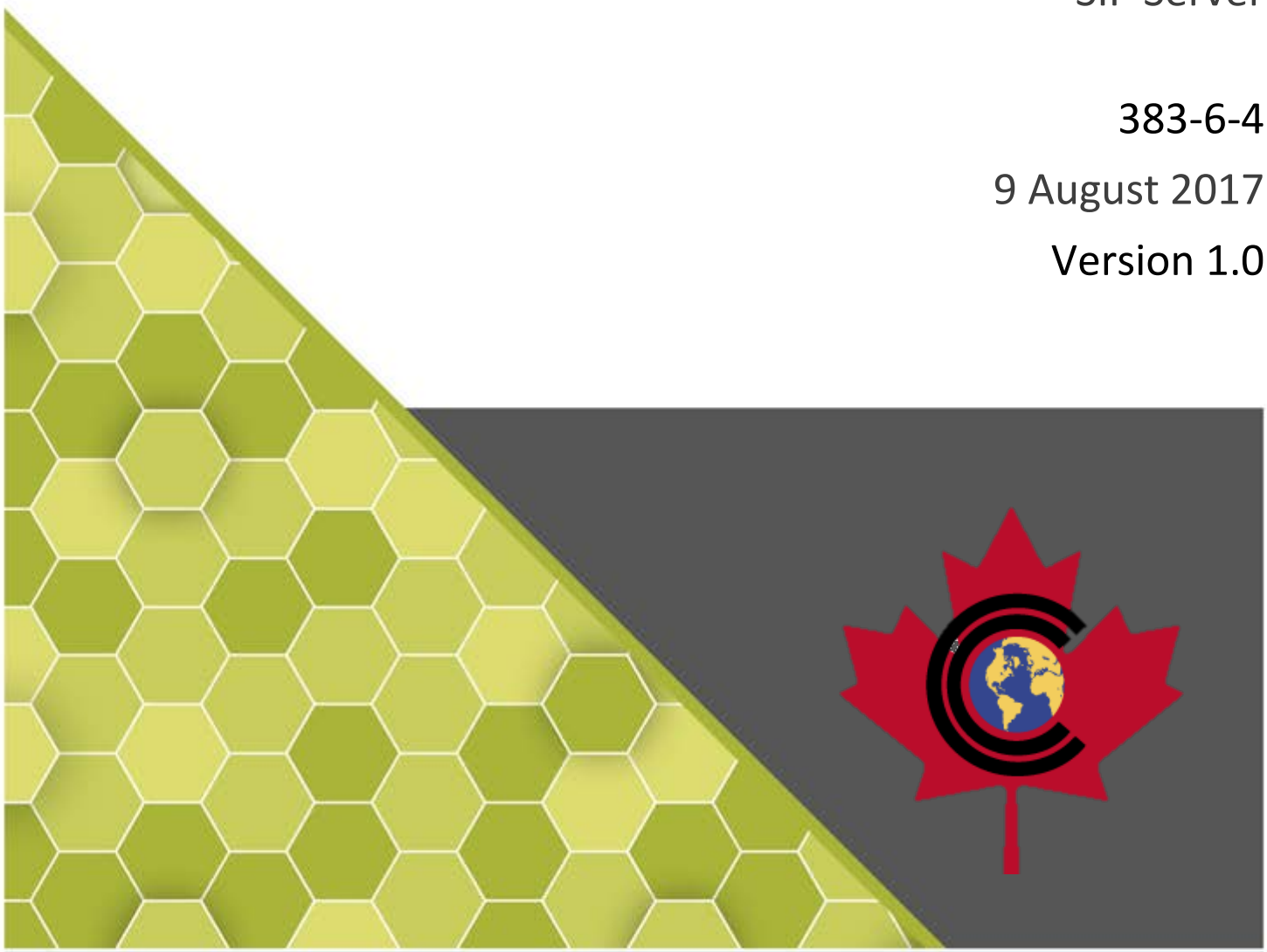
COMMON CRITERIA CERTIFICATION REPORT

Network Device collaborative Protection Profile Extended Package SIP Server

383-6-4

9 August 2017

Version 1.0



Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

EXECUTIVE SUMMARY

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the 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.

An evaluation of the Network Device collaborative Protection Profile Extended Package SIP Server was performed concurrently with the first product evaluation against the Extended Package's (EP) requirements. In this case the Target of Evaluation (TOE) was the Secusmart SecuSUITE SIP Server v1.0. The CCEF that carried out this evaluation is EWA-Canada and the evaluation was completed in May 2017.

TABLE OF CONTENTS

LIST OF TABLES

1 IDENTIFICATION OF TARGET OF EVALUATION

The Extended Package (EP) associated with this certification report is identified by the following nomenclature:

Table 1 EP Identification

EP Name	Network Device collaborative Protection Profile Extended Package SIP Server
Version	2.0
Date	December 01, 2015

1.1 COMMON CRITERIA CONFORMANCE

This EP conforms to Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4. It is CC Part 2 extended and CC Part 3 conformant.

1.2 EXTENDED PACKAGE DESCRIPTION

This Extended Package (EP) describes the security requirements for a Session Initiation Protocol (SIP) Server and provides a minimal baseline set of requirements targeted at mitigating well defined threats. The Voice over IP (VoIP) infrastructure for an enterprise can vary greatly, both in size and complexity. Many kinds of functionality are possible, often desirable, and sometimes necessary – including Session Border Controllers, gateways, trunking, Network Address Translation, and firewall traversal. The SIP Server interacts with a VoIP client and provides registrar and proxy capabilities required for call-session management as well as establishing, processing, and terminating VoIP calls. As a registered server, 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.

This EP is not complete in itself, but rather extends the collaborative Protection Profile for Network Devices (NDcPP). Since this EP builds on the NDcPP, conformant TOEs are obligated to implement the functionality required in the NDcPP along with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein.

2 SECURITY PROBLEM DESCRIPTION AND OBJECTIVES

2.1 ASSUMPTIONS

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

- A.NO_GENERAL_PURPOSE - It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- A.PHYSICAL - Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- A.TRUSTED_ADMIN - TOE - Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

2.2 THREATS

A TOE that conforms to this EP shall be able the counter the following threats:

- T.ADMIN_ERROR - An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- T.TSF_FAILURE - Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- T.UNDETECTED_ACTIONS - Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- T.UNAUTHORIZED_ACCESS - A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- T.UNAUTHORIZED_UPDATE -A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- T.USER_DATA_REUSE - User data may be inadvertently sent to a destination not intended by the original sender.

2.3 SECURITY OBJECTIVES

A TOE that conforms to this EP shall be capable of satisfying the following security objectives:

- O.PROTECTED_COMMUNICATIONS - The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

- O.VERIFIABLE_UPDATES - The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
- O.SYSTEM_MONITORING - The TOE will provide the capability to generate audit data and send those data to an external IT entity.
- O.DISPLAY_BANNER - The TOE will display an advisory warning regarding use of the TOE.
- O.TOE_ADMINISTRATION - The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
- O.RESIDUAL_INFORMATION_CLEARING - The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
- O.SESSION_LOCK - The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
- O.TSF_SELF_TEST- The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

2.4 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The following contains objectives for the Operational Environment.

- OE.NO_GENERAL_PURPOSE - There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- OE.PHYSICAL - Physical security, commensurate with the value of the TOE and the data it contains, is providedby the environment.
- OE.TRUSTED_ADMIN - TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3 REQUIREMENTS

The EP contains baseline requirements (those that must be performed by the TOE or its underlying platform) and one additional requirement based on selections in the body of the EP. If certain selections are made, then additional requirement is required.

The following table contains the base requirements required by the EP.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1 Audit Data Generation
FCS: Cryptographic Support	FCS_TLSS_EXT.2 TLS Server Protocol with Mutual Authentication
FIA: Identification and Authentication	FIA_SIPS_EXT.1 Session Initiation Protocol (SIP) Server
FMT: Security Management	FMT_MTD.1/AdminAct Management of TSF Data
FMT: Security Management	FMT_SMF.1 Specification of Management Functions
FPT: Protection of the TSF	FPT_TUD_EXT.1 Extended: Trusted Update
FTP: Trusted Path/Channels	FTP_ITC.1(2) Inter-TSF Trusted Channel (TLS/SIP)
FTP: Trusted Path/Channels	FTP_ITC.1(3) Inter-TSF Trusted Channel (Protection from Modification or Disclosure –SIP Server)

The following table contains an additional requirement based on selections in the body of the EP. If certain selections are made, then the following additional requirement will need to be included.

Requirement Class	Requirement Component
Cryptographic Support	FCS_DTLS_EXT.1 Extended: Datagram Transport Level Security

4 ASSURANCE REQUIREMENTS

It is important to note that a TOE that is evaluated against this EP is inherently evaluated against the NDcPP as well. The NDcPP includes a number of Assurance Activities associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this EP includes a number of SFR-based Assurance Activities that refine the SARs associated with the EAL identified in the NDcPP. The assurance activities associated with SARs that are prescribed by the NDcPP are performed against the entire TOE (i.e. the portion that is addressed by the NDcPP as well as the portion that is addressed by this EP).

5 EVALUATION RESULTS

The requirements of this EP were certified as a result of the successful application of this EP, in conjunction with NDcPP v1.0, to the evaluation of the Secusmart SecuSUITE SIP Server v1.0 product. Since this EP builds upon the requirements of the NDcPP, the certification of this EP also took into account the previous validation of the NDcPP, as documented in Validation Report Collaborative Protection Profile for Network Devices, Version 1.0, February 27, 2015.

6 SUPPORTING CONTENT

6.1 LIST OF ABBREVIATIONS

Term	Definition
CCEF	Common Criteria Evaluation Facility
CSE	Communications Security Establishment
EP	Extended Package
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
NDcPP	Network Device Collaborative Protection Profile
PALCAN	Program for the Accreditation of Laboratories – Canada
SIP	Session Initiation Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
VoIP	Voice Over Internet Protocol

6.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Network Device collaborative Protection Profile Extended Package SIP Server, Version 2.0, December 01, 2015.
Collaborative Protection Profile for Network Devices, Version 1.0, February 27, 2015.
Validation Report Collaborative Protection Profile for Network Devices, Version 1.0, February 27, 2015.
Secusmart SecuSUITE SIP Server v1.0 Security Target, Version 1.7, May 2017.
Evaluation Technical Report for NDcPP with SIP_EP of Secusmart SecuSUITE SIP Server v1.0, Version 1.4, May 10, 2017.
Common Criteria Certification Report Secusmart SecuSUITE SIP Server v1.0, Version 1.0, May 10, 2017.