

Certification Report

Voltage SecureData Appliance 7.0.2

Sponsor and developer: **OpenText Inc.**
275 Frank Tompa Drive
Waterloo ON N2L 0A1
Canada

Evaluation facility: **SGS Brightsight B.V.**
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2400068-01-CR**

Report version: **1.0**

Project number: **NSCIB-2400068-01**

Author(s): **Brian Smithson**

Date: **03 November 2025**

Number of pages: **11**

Number of appendices: **0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	6
2.3.1 Assumptions	6
2.3.2 Clarification of scope	6
2.4 Architectural Information	7
2.5 Documentation	7
2.6 IT Product Testing	7
2.6.1 Testing approach and depth	7
2.6.2 Independent penetration testing	8
2.6.3 Test configuration	8
2.6.4 Test results	8
2.7 Reused Evaluation Results	8
2.8 Evaluated Configuration	8
2.9 Evaluation Results	8
2.10 Comments/Recommendations	9
3 Security Target	10
4 Definitions	10
5 Bibliography	11

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, 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 or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see <http://www.commoncriteriaportal.org>.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see <https://www.sogis.eu>.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Voltage SecureData Appliance 7.0.2. The developer of the Voltage SecureData Appliance 7.0.2 is OpenText Inc. located in Waterloo, ON, Canada and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE, Voltage SecureData Appliance 7.0.2 (SDA), is a Software TOE only and it provides protection of sensitive data, such as credit card numbers and Social Security numbers, stored in databases and applications. It enables enterprises to ensure that sensitive data residing in databases and used in applications is protected as it is collected, used, stored, and distributed to less controlled environments. SDA provides the ability to implement a comprehensive solution for data protection offering data de-identification, data masking, and data redaction that requires minimal changes to the underlying systems.

The Simple API provides a set of functions that are callable from existing C, C#.NET, and Java applications, enabling data protection functionality to be included into any such application and applications to communicate with the SDA to obtain keys.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2025-11-03 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security [NSCIB].

The scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the Voltage SecureData Appliance 7.0.2, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Voltage SecureData Appliance 7.0.2 are advised to verify that their own environment is consistent with 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 the TOE meets the EAL3: augmented (EAL3+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.3 (Systematic Flaw Remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 [CEM] for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [CC] (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

¹ The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Voltage SecureData Appliance 7.0.2 from OpenText Inc. located in Waterloo, ON, Canada.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Voltage SecureData Appliance (SDA)	7.0.2
Software (included in SDA)	Simple API	6.22.02

To ensure secure usage a set of guidance documents is provided, together with the Voltage SecureData Appliance 7.0.2. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE, Voltage SecureData Appliance 7.0.2 (SDA), is a Software TOE only and it provides protection of sensitive data, such as credit card numbers and Social Security numbers, stored in databases and applications. It enables enterprises to ensure that sensitive data residing in databases and used in applications is protected as it is collected, used, stored, and distributed to less controlled environments. SDA provides the ability to implement a comprehensive solution for data protection offering data de-identification, data masking, and data redaction that requires minimal changes to the underlying systems. The Simple API provides a set of functions that are callable from existing C, C#.NET, and Java applications, enabling data protection functionality to be included into any such application and applications to communicate with the SDA to obtain keys.

To support its purpose, it provides the following security features:

- Cryptographic Support, including format-preserving and identity-based encryption schemes.
- Security Management
- User Data Protection
- Audit
- Identification and Authentication
- Access Control
- Trusted Paths for communication with clients

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

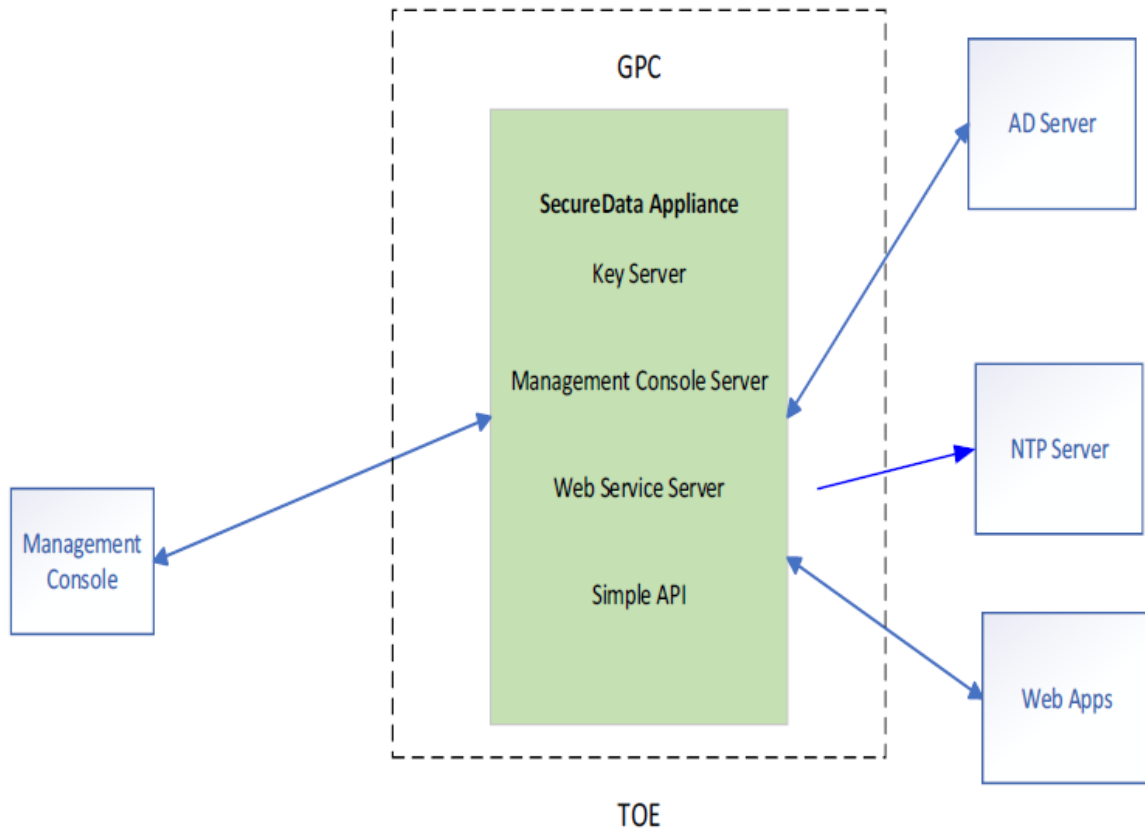
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the [ST].

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE is software-only. The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
SecureData Appliance, Software Version 7.0.2, Administrator Guide	April 2024
SecureData Appliance, Software Version 7.0.2 Installation Guide	April 2024
Common Criteria supplement, Voltage Secure Data Appliance 7.0.2, Operational Guidance and Installation Procedures	V0.7, September 2025

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The evaluator created additional test cases test to confirm verification of the version of the TOE / to supplement coverage of SFRs and/or TSFI / to further exercise the behaviour of critical functionality. Repeated developer tests were selected based on:

- The main functionalities of the TOE. Such as testing on the supported cryptographic functionality of the TOE.
- How much security relevant they are. Such as audit record protection from delete and modification.

The evaluator analysed the developer test plan against the SFRs and, based on the completeness of the tests, devised the evaluator test plan.

2.6.2 Independent penetration testing

Independent tests were chosen to cover:

- AGD_PRE.1.2 requirements.
- Negative test cases, such as tests that a non-administrator user performs activities that need administrators' privileges.
- Communication related SFRs such as:
 - IND.Test TLS for communication between SDA and LDAP server.
 - Verify secure initialization.
 - Nessus/NMAP scan.

The evaluator performed all the tests (independent tests and penetration tests) in the period between 13-05-2025 and 07-08-2025, with 40 man-week hours within two weeks were needed in total for testing and reporting. All of the test effort was on the logical tests.

2.6.3 Test configuration

The SDA can be used in a single server deployment or in a multiple server deployment. Only the single server deployment is being evaluated.

The TOE was tested in the following configurations:

- The SDA was tested on openSUSE Leap 15.5 on ESX 7.
- Chrome version used was 123 (also testes with Chrome version 124 and Firefox versions 123 and 124).
- TOE was configured for Authentication with both IP and credentials.
- This is the same configuration as stated in the ST.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the [ETR], with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its [ST] and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Voltage SecureData Appliance 7.0.2.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the [ETR], which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "Pass".

Based on the above evaluation results the evaluation lab concluded the Voltage SecureData Appliance 7.0.2, to be **CC Part 2 conformant**, **CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented with ALC_FLR.3**. This implies that the product satisfies the security requirements specified in Security Target [S7].

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: RFC 5091: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems; 1363.3-2013 - IEEE Standard for Identity-Based Cryptographic Techniques using Pairings; and P1619.2 – IEEE Standard for Wide-Block Encryption for Shared Storage Media, which are out of scope as there are no security claims relating to these.

3 Security Target

The Voltage SecureData Appliance 7.0.2 Security Target, v0.19, 5 September 2025 [ST] is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

- [CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
- [ETR] Evaluation Technical Report Voltage SecureData Appliance v7.0.2 – EAL3+, 24-RPT-1033, v2.0, 20 October 2025
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
- [ST] Voltage SecureData Appliance 7.0.2 Security Target, v0.19, 5 September 2025

(This is the end of this report.)