UNCLASSIFIED

TLP:WHITE

Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Vormetric Data Security Manager V6000, Version 6.3

7 October 2020

517 CCS 2020

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

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 Centre for Cyber Security (CCCS). This certification report, and its associated certificate, applies 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 Canadian CC Scheme, 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

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

Contact Centre and Information Services
Edward Drake Building
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

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 Canadian Centre for Cyber Security.

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, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the 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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Vormetric Data Security Manager V6000, Version 6.3 (hereafter referred to as the Target of Evaluation, or TOE), from Thales DIS CPL USA, Inc. , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

CygnaCom Solutions, Inc. is the CCEF that conducted the evaluation. This evaluation was completed on 7 October 2020 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance 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 Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian CC Scheme and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Vormetric Data Security Manager V6000, Version 6.3
Developer	Thales DIS CPL USA, Inc.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

The TOE claims the following conformance:

Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013

1.2 TOE DESCRIPTION

The TOE creates, stores, and manages policies that protect data residing on managed hosts. The TOE operates by integrating with an access control product, called Transparent Encryption Agent, installed on the host machines that contain protected data and to specify data access policies that are sent to these agents. Administrators access the TOE through a browser-based user interface.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

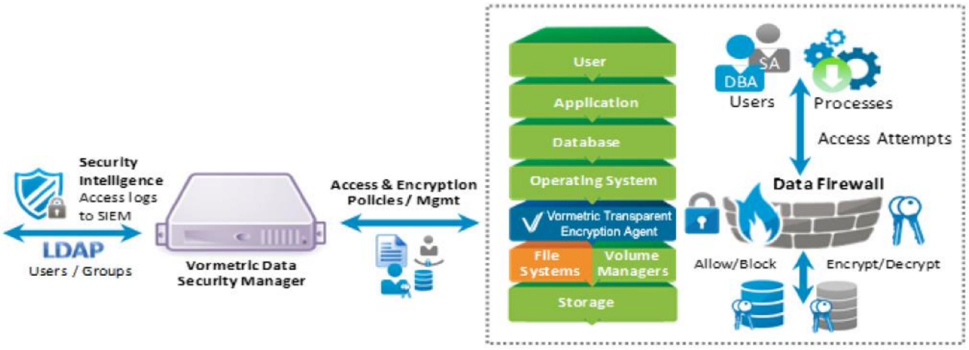

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- System Monitoring
- Robust TOE Access
- Authorized Management
- Policy Definition
- Dependent Product Configuration
- Confidential Communications
- Access Bannering
- Cryptographic Services

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations have been evaluated by the CAVP and are used by the TOE:

Table 2: Cryptographic Implementation(s)

Cryptographic Algorithm	Certificate Number
Vormetric Data Security Server Module v6.3.0	#C1377, #C1389

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE will be able to establish connectivity to other ESM products in order to share security data
- The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
- The TOE will receive reliable time data from the Operational Environment.
- The TOE will receive identity data from the Operational Environment.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.

3.2 CLARIFICATION OF SCOPE

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

Only the functionality included in the Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013 was evaluated.

The following TOE features were not evaluated/included in the scope of the evaluation:

1. The CLI should be only used for initial configuration and off-line maintenance.

2. CLI over SSH is not evaluated and must be disabled. Local CLI access is not evaluated and the DSM appliance must be physically secured.

3. VMSSC (An external Vormetric command line tool for administering the DSM) - VMSSC is a separate utility that is not part of the TOE distribution and must be installed separately. VMSSC is not included in the scope of the evaluation.

4. Transparent Encryption Agent – This is an external agent that is not a part of TOE distribution. The scope of testing is limited to the Transparent Encryption Agent successfully receiving and loading the policy.

5. SNMP service – Use of the SNMPv1 and SNMPv2 functionality is excluded and it is disabled by default. The use of SNMPv3 with read-only community strings is not restricted in the evaluated configuration; however, it is not evaluated.

6. IPMI – This service offers the same TOE off-line maintenance capability as CLI. IPMI can not be used to import or export DSM cryptographic keys. IPMI service should be disabled in the evaluated configuration.

7. Failover DSM – failover is not restricted in the evaluated configuration; however, it is not evaluated. Failover configuration is disabled by default. This interface uses standard database data replication method. When configured, the database replication does not transmit plaintext data.

8. Auto-backup via SCP and CIFS are not evaluated.

9. Application Encryption Agent – This is an external agent that is not a part of the TOE distribution. The agent functionality is not evaluated.

10. Key Agents for SQL and Oracle Database – These are external agents that are not a part of the TOE distribution. These two agents are not evaluated.

11. KMIP client – This is an external client that is not a part of the TOE distribution. This client is not evaluated.

12. Email notification – email notification is disabled by default. SMTP is not evaluated.

13. Optional RSA Authentication Manager is not evaluated.

14. Optional External Certificate Authority is not evaluated.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

The TOE firmware (Version 6.3 Build 14515) running on the V6000 DSM appliance, communication with one or more Vormetric Transparent Encryption Agents, with support from the operating environment for:

- NTP Server
- SMTP Server
- DNS Server
- LDAP Server
- RSA Authentication manager
- External Certificate Authority

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Vormetric Data Security Manager (DSM) Common Criteria Addendum, Version 1.2, July 23, 2020
b) Vormetric Data Security Platform DSM Administration Guide Release 6 Version v6.3.0 August 21, 2019 v2

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

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

6 TESTING ACTIVITIES

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

6.1 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 Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP

b. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementations are present in the TOE

6.3.1 FUNCTIONAL TEST RESULTS

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

6.4 INDEPENDENT PENETRATION TESTING

The penetration testing effort focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their penetration testing effort.

6.4.1 PENETRATION TEST RESULTS

Type 1 & 2 searches were conducted on 7/11/2020 and included the following search terms:

- smartmontools
- Irqbalance
- bash
- Java (Oracle Java 8)
- postgresql
- Wildfly
- Python
- OpenSSH
- OpenSSL
- crontabs
- authconfig
- bind
- bzip2
- ca-certificates
- checkpolicy
- cpp
- dbus
- device-mapper
- dhclient
- dos2unix
- dracut
- e2fsprogs
- elfutils
- ethtool
- expect
- systemd
- rsyslog
- gettext
- glib2
- gnupg2
- grep
- grub2
- gzip
- hostname
- iproute
- ipset
- iptables
- iputils
- json-c
- langtable
- logrotate
- mailx
- microcode_ctl
- nmap-ncat
- ntp
- ntpdate
- openIPMI-modalias
- openldap
- passwd
- pciutils
- pcre
- policycoreutils
- rpm
- rsync
- samba-client
- sed
- shared-mime-info
- slang
- sqlite
- sudo
- tar
- tcl
- traceroute
- unixODBC
- unzip
- util-linux
- vim-common
- which
- yum
- zip

Vulnerability searches were conducted using the following sources:

- National Vulnerability Database (https://nvd.nist.gov/vuln/search)
- Open Sourced Vulnerability Database (https://www.cvedetails.com/product-search.php)

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

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 Centre for Cyber Security (CCCS). This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 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.
Evaluation Technical Report Vormetric Data Security Manager V6000, Version 6.3, 7 October 2020, v1.1
Security Target Vormetric Data Security Manager V6000, Version 6.3, 7 October 2020, v3.3
Assurance Activity Report Vormetric Data Security Manager V6000, Version 6.3, 7 October 2020, v1.1