Certification Report

EAL 2+ Evaluation of EMC® Symmetrix® VMAX™ Series with Enginuity™ Operating Environment 5875, Solutions Enabler 7.2.0 and Symmetrix Management Console 7.2.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-139-CR
Version: 1.0
Date: 2 March 2011
Pagination: i to iii, 1 to 10

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, 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 2 March 2011, 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 registered trademarks:

- Symmetrix, Symmetrix VMAX Series with Enginuity, and EMC are registered trademarks of EMC Corporation.

TABLE OF CONTENTS

Executive Summary

EMC® Symmetrix® VMAX™ Series with Enginuity™ Operating Environment 5875, Solutions Enabler 7.2.0 and Symmetrix Management Console 7.2.0 (hereafter referred to as Symmetrix VMAX Series), from EMC Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Symmetrix VMAX Series is a software application that provides data access control for mid- to high-end data storage systems. The Enginuity component runs on a Symmetrix hardware platform and services requests to the data store; the Solutions Enabler[1] and Symmetrix Management Console[2] components run on a separate workstation providing management interfaces to the Enginuity component. Data storage systems can range in size from hundreds of terabytes to petabytes, and can be composed of high-capacity magnetic disk drives or high-speed solid state drives. Stored data is zeroized before disk space is reallocated.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 10 February 2011 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 Symmetrix VMAX Series, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the 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)[3] 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 augmentation is claimed: ALC_FLR.2 – Flaw reporting procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Symmetrix VMAX Series evaluation meets all the conditions of the *Arrangement on*

---

[1] Solutions Enabler is a Command Line Interface (CLI) and Application Programming Interface (API).

[2] Symmetrix Management Console is a web-based Graphical User Interface (GUI).

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

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   Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is EMC® Symmetrix® VMAX™ Series with Enginuity™ Operating Environment 5875, Solutions Enabler 7.2.0 and Symmetrix Management Console 7.2.0 (hereafter referred to as Symmetrix VMAX Series), from EMC Corporation.

2   TOE Description

Symmetrix VMAX Series is a software application that provides data access control for mid-to high-end data storage systems. The Enginuity component runs on a Symmetrix hardware platform and services requests to the data store; the Solutions Enabler[4] and Symmetrix Management Console[5] components run on a separate workstation providing management interfaces to the Enginuity component. Data storage systems can range in size from hundreds of terabytes to petabytes, and can be composed of high-capacity magnetic disk drives or high-speed solid state drives. Stored data is zeroized before disk space is reallocated.

3   Evaluated Security Functionality

The complete list of evaluated security functionality for Symmetrix VMAX Series is identified in Section 6 of the Security Target (ST).

4   Security Target

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

Title: EMC Corporation EMC® Symmetrix® VMAX™ Series with Enginuity™
          Operating Environment 5875, Solutions Enabler 7.2.0, and Symmetrix
          Management Console 7.2.0
Version: 0.7
Date: 26 January 2011

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*.

Symmetrix VMAX Series is:

---

[4] Solutions Enabler is a Command Line Interface (CLI) and Application Programming Interface (API).

[5] Symmetrix Management Console is a web-based Graphical User Interface (GUI).

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, as well as the following: ALC_FLR.2 – Flaw reporting procedures.

6   Security Policy

Symmetrix VMAX Series implements a Discretionary Access Control policy over devices attempting to manage or configure the protected data storage, and a Storage Access Control Policy on devices trying to read to or write from the protected data storage.

In addition, Symmetrix VMAX Series implements policies pertaining to security audit, user data protection, identification and authentication, and security management.

Further details on these security policies may be found in Section 6 of the ST.

7   Assumptions and Clarification of Scope

Consumers of Symmetrix VMAX Series 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:

a. There are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and

b. Administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.

7.2   Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. The TOE is located within a controlled access facility and is physically available to authorized administrators only;

b. The IT Environment blocks all traffic originating from outside of the controlled access facility intended for the Solutions Enabler ports of the TOE;

c. The IT Environment will provide reliable timestamps for the TOE to use; and

d.   The IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.

7.3   Clarification of Scope

Symmetrix VMAX Series is not intended to be placed or operated in a hostile environment, and should be protected by other products specifically designed to address sophisticated threats.

8   Evaluated Configuration

The evaluated configuration for Symmetrix VMAX Series comprises: Enginuity™ Operating Environment 5875.151, Solutions Enabler 7.2.0, and Symmetrix Management Console 7.2.0.

The Symmetrix VMAX Series requires Symmetrix hardware provided by EMC Corporation for the Enginuity component, a Storage Area Network (SAN) to allow devices to connect to Symmetrix VMAX Series, devices on the network that use the storage that the Symmetrix VMAX Series provides, cables and connectors that allow the devices to connect to the SAN, and an administrator workstation with an operating system that supports Solutions Enabler and Symmetrix Management Console.

ST Section 1.4.1 provides additional Symmetrix VMAX Series deployment detail; ST Table 2 provides a comprehensive list of Solutions Enabler and Symmetrix Management Console supported operating systems.

9   Documentation

The EMC documents provided to the consumer are as follows:

a.   Symmetrix Solutions Enabler Release Notes;

b.   Symmetrix Management Console Release Notes;

c.   Symmetrix VMAX Series Release Notes;

d.   Symmetrix VMAX Series Product Guide;

e.   Symmetrix VMAX Series Physical Planning Guide;

f.   Symmetrix Management Console Online Help;

g.   Symmetrix Management Console Installation Guide;

h.   Solutions Enabler Symmetrix CLI Quick Reference;

i.   Solutions Enabler Symmetrix CLI Command Reference; and

j.   Solutions Enabler Installation Guide.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Symmetrix VMAX Series, including the following areas:

Development: The evaluators analyzed the Symmetrix VMAX Series 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 Symmetrix VMAX Series security architectural description and determined that the initialization process is secure and 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 is correct.

Guidance Documents: The evaluators examined the Symmetrix VMAX Series 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 Symmetrix VMAX Series configuration management system and associated documentation was performed. The evaluators found that the Symmetrix VMAX Series configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well developed.

The evaluator examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Symmetrix VMAX Series during distribution to the consumer.

The evaluator reviewed the flaw remediation procedures used by EMC for Symmetrix VMAX Series. During a site visit, the evaluator examined the evidence generated by adherence to the procedures. The evaluator concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Symmetrix VMAX Series. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Symmetrix VMAX Series potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the Symmetrix VMAX Series 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[6].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design 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 was the following list of EWA-Canada test goals:

a. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance; and

b. Repeat of Developer's Tests: The objective of this test goal is to repeat the developer's tests on the evaluator's TOE installation.

---

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

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 that focussed on attempting to gain access to management accounts through direct attack.

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

11.4 **Conduct of Testing**

Symmetrix VMAX Series was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the EMC Corporation facility in Hopkinton, MA. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Procedures and Test Results document.

11.5 **Testing Results**

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Symmetrix VMAX Series behaves as specified in its ST, functional specification, TOE design, and security architecture description.

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 developer has an extensive and robust automated test suite capable of insuring a proper working product.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
API	Application Programming Interface
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list

Acronym/Abbreviation/ Initialization	Description
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
SAN	Storage Area Network
ST	Security Target
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.   EMC Corporation EMC® Symmetrix® VMAX™ Series with Enginuity™ Operating
        Environment 5875, Solutions, Version 0.7, 26 January 2011.

e.   Evaluation Technical Report (ETR) for EAL3+ Common Criteria Evaluation of
        EMC® Symmetrix® VMAX™ Series with Enginuity™ Operating Environment
        5875, Solutions Enabler 7.2.0 and Symmetrix Management Console 7.2.0 , Document
        No. 1640-000-D002, Version 1.3, 10 February 2011, Common Criteria Evaluation
        Number: 383-4-139.