C088 Certification Report

Micro Focus Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10

File name: ISCB-5-RPT-C088-CR-v1
Version: v1
Date of document: 20 December 2017
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C088 Certification Report

Micro Focus Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10

20 December 2017

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 □Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C088 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C088-CR-v1
ISSUE:	v1
DATE:	20 December 2017

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright and Confidentiality Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB 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 20 December 2017 and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). 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 MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	5 December 2017	All	Initial draft of certification report
d2	13 December 2017	All	2nd draft of certification report
v1	20 December 2017	All	Final certification report

Executive Summary

The Target of Evaluation (TOE) is Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10 from Micro Focus.

The TOE provides protection of sensitive data, such as credit card numbers and Social Security numbers. 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 SecureData Simple API provides a set of functions that are callable from existing C, C#/.NET, and Java applications. It allows data protection functionality to be included into any such application and enables applications to communicate with the SDA to obtain keys.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented ALC_FLR.1. This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 29 November 2017.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

The TOE, Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10, has been rebranded from Hewlett Packard Enterprise (HPE) to Micro Focus. All HPE guidance documentation is effectively in the process of being renamed to Micro Focus and the contents of the documents themselves remain unchanged and are applicable to the TOE.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The TOE is Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10 from Micro Focus. The TOE 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.

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

3 The functionality defined in the Security Target (Ref [6]) that was subsequently evaluated is as follows:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification & Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

1.2 TOE Identification

4 The details of the TOE are identified in

5 Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C088
TOE Name	Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10
TOE Version	SDA v6.4 and SecureData Simple API v5.10

Security Target Title	Voltage SecureData Appliance and SecureData Simple API Security Target
Security Target Version	Version 1.0
Security Target Date	1 November 2017
Assurance Level	Evaluation Assurance Level 2 Augmented ALC_FLR.1
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 2 with Augmented ALC_FLR.1
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046
Developer	Micro Focus 1140 Enterprise Way, Sunnyvale CA, 94089
Evaluation Facility	BAE Systems Applied Intelligence – MySEF (Malaysia Security Evaluation Facility) Level 28, Menara Binjai, 2 Jalan Binjai, 50450 Kuala Lumpur, Malaysia

1.3 Security Policy

6 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

7 The TOE includes both logical and physical boundaries as described in Section 2.5 and 2.6 of the Security Target (Ref [6]).

8 The TOE architecture consists of the following components:

1) Key Management Server:

   The Key Management Server supports centralized Voltage SecureData key management. Voltage SecureData is built around a centralized key management system that coordinates the generation and issuance of FPE keys, AES keys, and IBE keys. Unlike traditional systems using randomly generated keys that require complex backup and recovery procedures, the Key Management Server provides stateless key generation through the use of a Key Derivation Function (KDF).

2) Management Console:

The Management Console provides a web-based interface to support centralized configuration and reporting across the Voltage SecureData solution.

3) Web Service Server (SOAP and REST APIs):

The Web Service Server provides a data protection interface that can be used by web applications capable of consuming WSDL information. Web Services are an industry standard method of integrating applications with external services. Web implementations are available in a diverse set of application platforms from web browsers to mainframes. The Web Service allows practically any application to make use of the functionality in Voltage SecureData.

4) SecureData Simple API:

The SecureData Simple API client provides a set of functions that are callable from existing C, C#, and Java applications. The SecureData Simple API allows users to include data protection functionality in their applications, and to communicate with the Key Management Server to obtain keys.

9 The TOE supports a number of different deployment architectures, but they can essentially be characterized as follows:

i. A single-server system that includes all SDA components on one computer:

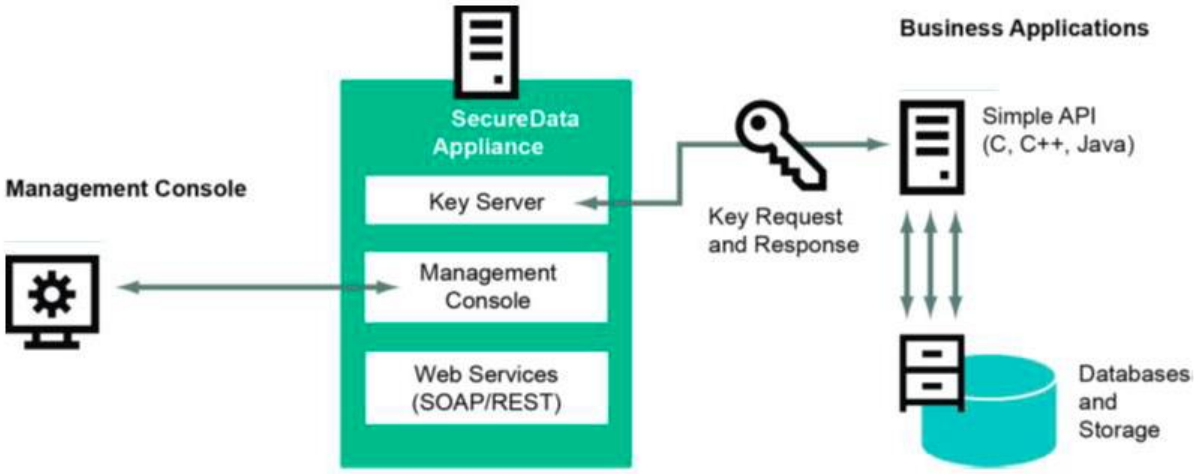

Figure 1: Example Single-Server Deployment

In a single-server system, the Management Console, Key Server, and Web Services Server are installed together on a single server.

ii. A multi-server system that distributes SDA components among at least two computers:

A multi-server system includes multiple servers that are managed from a single Management Console. In a multi-server system, the Management Console, Key Server, and Web Service Server can all be placed on separate servers.

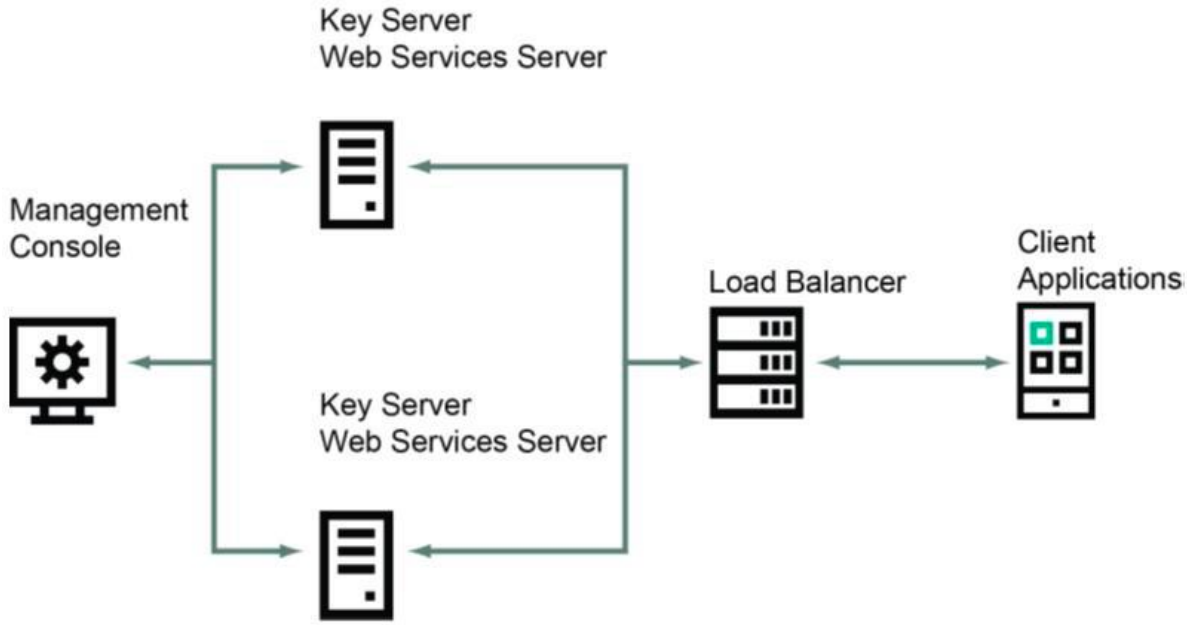

Figure 2: Example Multi-Server Deployment

10 The TOE includes the following components:

I. Key Management Server

II. Management Console

III. Web Services Server (SOAP and REST APIs)

IV. SecureData Simple API

1.4.1 Logical Boundaries

11 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

12 **Audit:** The TOE is able to generate audit records of security relevant and other events as they occur, including: starting and stopping the audit function; all use of user identification and authentication mechanisms; and all use of management functions.

Generated audit records include the following information: date and time of the event; type of event; subject identity; and a description of the event and its outcome. Generated audit events resulting from the actions of identified users include the identity of the user that caused the event.

Generated audit records are stored in a database and protected from unauthorized deletion. The audit records are digitally signed and the TOE is able to detect if stored audit records have been modified. The TOE provides authorized users with the capability to read audit information from the audit records. The audit records are displayed in a manner suitable for the authorized user to interpret the information. The TOE provides capabilities to search audit data for review based on specified search criteria and to select audit data for review based on time interval, audit record fields and specific values of selected fields.

13 **Cryptographic Support:** The TOE provides implementations of the following cryptographic capabilities: Format Preserving Encryption (FPE); embedded Format Preserving Encryption (eFPE); Identity-Based Encryption (IBE); and Identity-Based Symmetric Encryption (IBSE). In support of these capabilities, the TOE generates master keys from which encryption keys are derived and destroys master keys when they are no longer required.

14 **User Data Protection:** The TOE enforces an access control policy on Web Service clients that authorizes clients to perform protection and access operations on data based on the client's identity, authentication credentials, and IP address.

15 **Identification and Authentication:** The users of the TOE comprise administrators, who manage the TOE and its configuration, and clients, who request key management services from the TOE.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords and enforces minimum requirements for the construction of administrator passwords. Additionally, the TOE can be configured to use an LDAP directory to support remote user authentication. Once configured, any user belonging to the specified LDAP group(s) is granted automatic login access to the Management Console without having to explicitly create a local account for that user.

When the TOE receives client requests for encryption or decryption keys, the clients must first be authenticated. The administrator configures one or more authentication methods for a district. An authentication method defines rules for authenticating the identity of a key requester, including identity patterns, IP addresses, and the type of authentication. The TOE supports the following client authentication types in its evaluated configuration: shared secret; LDAP username and password; certificate.

16 **Security Management:** The SDA implements two management interfaces—the Appliance Menu, which is used for initial configuration of the SDA, and the Management Console, which provides the capabilities necessary to manage the TOE security functionality.

17 **Protection of the TSF**: When the TOE is configured as a multi-server system, communications between distributed components of the TOE occur over TLS, which provides confidentiality and integrity of transmitted data. In addition, the Simple API client software communicates with the SDA over TLS.

The SDA includes a Linux-based operating system that provides a reliable time stamp derived from the hardware clock of the computer on which the SDA software is installed. The system time can be set manually by an administrator via the Appliance Menu, or the SDA can be configured to synchronize its clock using NTP.

18 **TOE Access:** The TOE will terminate interactive sessions after 15 minutes of inactivity. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off. The TOE can be configured to limit remote access to IP addresses matching administrator-configured IP addresses or address patterns.

19 **Trusted Path/Channels:** The TOE provides a trusted channel to communicate securely with SecureData clients in the operational environment. The trusted channel is implemented using TLS, which ensures all communication over the channel is protected from disclosure and modification.

The TOE provides a trusted path for administrators to communicate with the TOE. The trusted path is implemented using HTTPS (i.e., TLS over HTTP) for access to the Management Console and SSH for remote access to the Appliance Menu. The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS and SSH ensures all communication over the trusted path is protected from disclosure and modification.

1.5 Clarification of Scope

20 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

21 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

22 The following features and capabilities of the TOE described in the guidance documentation are not included within the scope of the evaluation:

- KMS for Hadoop TDE (outside TOE boundary)
- Web Front End Server (outside TOE boundary)

23 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirement for using functions and services outside of the evaluated configuration.

1.6 Assumptions

24 This section summarises the assumptions regarding the operational environment and the intended usage of the TOE, as described in the Security Target (Ref [6]):

a) There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

b) The TOE software critical to security policy enforcement will be protected from unauthorised physical modification.

1.7 Evaluated Configuration

25 As stated in the ST (Ref [6]), there are four (4) main components of the TOE that make up the evaluated configuration, namely the Management Console, Key Management Server, Web Service Server (SOAP and REST APIs) and SecureData Simple API.

26 The TOE components are deployed either as a single-server or a multi-server environment in an enterprise network. The Management Console component of the TOE provides a web-based interface to support centralised configuration and reporting across the Voltage SecureData solution. The Key Management Server supports centralised Voltage SecureData key management. Voltage SecureData is built around a centralised key management system that coordinates the generation and issuance of FPE keys, AES keys, and IBE keys. The

Web Service Server provides an application programming interface (API) for protecting and accessing data. It also provides specialised operations for protecting and accessing commonly used data formats, such as credit card numbers and Social Security numbers, and it provides array interfaces to FPE calls in order to optimise the performance of batch operations. The SecureData Simple API provides a set of functions that are callable from existing C, C#/.NET, and Java applications. It allows data protection functionality to be included into any such application and enables applications to communicate with the SDA to obtain keys.

27 The SDA also includes the following components during the installation process that are outside the TOE boundary:

- Web Front End Server (FES)
- KMS for Hadoop TDE

28 The evaluated configuration requires that all communications between distributed components of the TOE occur over TLS, which provides confidentiality and integrity of transmitted data. The TOE can be configured in either of two modes: non-FIPS mode and FIPS 140-2 compliant mode. However, the evaluated configuration mode of operation is non-FIPS as FIPS mode limits client access to only the REST API, as stated in the ST (Ref. [6]).

29 The TOE supports the following components in the operational environment; however, they are not required in the evaluated configuration:

- NTP server to provide time synchronisation to the TOE platform
- LDAP server to support user authentication
- HSM to support storage of root keys

1.8 Delivery Procedures

30 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

31 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

32 The TOE delivery procedures are as follows:

- Product Orders: A customer contacts Micro Focus – Data Security Sales to identify and purchase a SecureData deployment of the TOE that is suitable to meet the customer's needs. Contact can be made via the Micro Focus – Data Security Contact Sales page or telephone. When Micro Focus Voltage receives an order for a product, the Voltage

Support team will be notified to trigger the creation of a Voltage Downloads Portal account for the customer. The Portal provides customers access to the product, manual, and updates.

- TOE Download: The Voltage Downloads Portal (https://downloads.voltage.com/) will be used to download the software, updates, and manuals. Micro Focus Voltage Customer Support will be notified when a customer purchases the SDA or Simple API, and will create a Voltage Downloads Portal account for the customer. Access is granted for up to 6 users per customer. An email will be sent to the customer after the account has been created. Customers log in using the provided credentials and are encouraged to change the password. If an existing customer is purchasing additional options, Voltage Customer Support will simply provide the customer access to the options or products they have purchased.

33 All delivery process details are described in Section 4 of the Life Cycle documentation.

1.9 Documentation

34 It is important that the TOE is used in accordance with the guidance documentation in order to ensure secure usage of the product.

The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product. Note: All Hewlett Packard Enterprise (HPE) guidance documentation is effectively in process of being renamed to Micro Focus. The contents of the documents are unaffected by the naming change.

- SecureData Appliance Version 6.4 Release Notes, October 2017
- HPE SecureData Administrator Guide, version 6.4, October 2017
- HPE SecureData Architecture Guide, version 6.4, October 2017
- HPE SecureData Atalla HSM Supplement, version 6.4, October 2017
- HPE SecureData Appliance Installation Guide, version 6.4, October 2017
- HPE SecureData REST API Developer Guide, version 6.4, October 2017
- HPE SecureData SOAP API Developer Guide, version 6.4 October 2017
- HPE SecureData Simple API Developer Guide Version 5.10, May 2017
- HPE SecureData Simple API Installation Guide Version 5.10, May 2017

2 Evaluation

35 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [4]).

2.1 Evaluation Analysis Activities

36 The evaluation activities involved a structured evaluation of the TOE, including the following components:

- The evaluators' testing consisted of independent testing efforts, which comprise both functional and penetration test cases to address testing requirements for ATE_IND.2 and AVA_VAN.2 evaluation components.
- For functional testing, the focus was on testing the claimed security functionality (SFRs within the ST) through the interfaces specified in the functional specification (TSFI). For the penetration testing, the effort was limited to attacks that are commensurate to an attacker with equal or less than Basic attack potential. The testing approach for both testing commensurate with the respective assurance components (ATE_IND.2 and AVA_VAN.2).

2.1.1 Life-cycle support

2.1.1.1 Configuration Management Capability

37 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

38 The evaluators confirmed that the TOE references used are consistent.

39 The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

40 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

2.1.1.2 Configuration Management Scope

41 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;
- the parts that comprise the TOE; and
- the evaluation evidence required by the SARs in the ST.

42 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

43 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.1.3 TOE Delivery

44 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

2.1.1.4 Basic Flaw Remediation

45 The evaluator examined the flaw remediation procedures documentation and determined that it describes the procedures used to track all reported security flaws in each release of the TOE.

46 The evaluator examined the flaw remediation procedures and determined that the application of these procedures would produce a description of each security flaw in terms of its nature and effects.

47 The evaluator examined the flaw remediation procedures and determined that the application of these procedures would identify the status of finding a correction to each security flaw.

48 The evaluator checked the flaw remediation procedures and determined that the application of these procedures would identify the corrective action for each security flaw.

49 The evaluator examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information on each security flaw.

2.1.2 Development

2.1.2.1 Architecture

50 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

51 The security architecture description describes the security domains maintained by the TSF.

52 The initialisation process described in the security architecture description preserves security.

53 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

2.1.2.2 Functional Specification

54 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given,

55 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI,

56 The evaluators also confirmed that the developer supplied tracing that links the SFRs to the corresponding TSFIs.

2.1.2.3 TOE Design Specification

57 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

58 The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

59 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

60 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

61 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

62 The evaluators determined that all SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operational Guidance

63 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

64 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

65 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

66 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

67 The evaluators found that the operational user guidance is clear and reasonable.

2.1.3.2 Preparation Guidance

68 The evaluators examined the provided delivery acceptance documentation and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

69 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

70 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

71 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and conducting penetration tests. The TOE testing was conducted by the evaluators of BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Assessment of Developer Tests

72 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

2.1.4.2 Independent Functional Testing

73 At EAL2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan and creating test cases that are independent of the developer's tests.

74 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Test ID	Description	SFRs
TEST-IND-001-APP	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that authorised users are able to perform management of TSF data functions. • Verify that authorised users are able to determine and modify the behaviour of security management functions. • Verify that the TSF shall maintain security roles. • Verify that the TSF data is protected from	FIA_ATD.1.1, FIA_SOS.1.1 , FIA_UAU.2.1, FIA_UAU.5.1, FIA_UID.2.1, FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_STM.1.1, FTA_SSL.4, FTP_TRP.1.1, FTP_TRP.1.2,

Test ID	Description	SFRs
	disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels. • Verify that the TSF is able to provide reliable timestamps.	FTP_TRP.1.3
TEST-IND-002-MC	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that authorised users are able to perform management of TSF data functions. • Verify that authorised users are able to determine and modify the behaviour of security management functions. • Verify that authorised users are able to manage the rules used in enforcing the Access Control policy on Web Service clients and that the TSF provides restrictive default values or specifies alternative values to override the default settings. • Verify that the TSF shall maintain security roles. • Verify that the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels. • Verify that the TSF generates audit records for auditable events and provides a means for authorised users to view the audit logs and provides reliable timestamps.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1, FAU_SAR.1.2, FCS_CKM.1.1(1), FCS_CKM.1.1(2), FCS_CKM.4.1, FIA_ATD.1.1, FIA_SOS.1.1, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UID.2.1, FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2, FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_STM.1.1, FTA_SSL.4.1, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3
TEST-IND-003-MC	• Verify that the TSF performs TOE access functions such as user session termination and inactive session termination. • Verify that the TSF is able to deny session establishment based on the IP address of the source of a session request. • Verify that the TOE generates audit records for auditable events and provides a means for authorised users to view the audit logs. • Verify that the TSF restricts access to audit records, provides the capability to select and order audit records and protects audit records from unauthorised deletion and modification.	FTA_TSE.1.1, FTA_SSL.3.1, FAU_SAR.3.1, FAU_STG.1.1, FAU_STG.1.2

Test ID	Description	SFRs
TEST-IND-004-SOAP	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that the TSF is able to perform cryptographic operations based on the keys defined. • Verify that the TSF is able to enforce access control policy on Web Service clients that authorises clients to perform protection and access operations on data, based on the client's identity, authentication credentials, and IP address. • Verify that the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels. • Verify that the TOE generates audit records for auditable events and provides a means for authorised users to view the audit logs.	FAU_GEN.1.1, FAU_GEN.1.2, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UID.2.1, FCS_CKM.1.1(1), FCS_CKM.1.1(2), FCS_COP.1.1(1), FCS_COP.1.1(2) , FDP_ACC.1.1, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4, FPT_ITT.1.1, FTP_ITC.1.1, FTP_ITC.1.2, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3
TEST-IND-005-SIMPLE	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that the TSF is able to perform cryptographic operations based on the keys defined. • Verify that the TSF is able to enforce access control policy on Web Service clients that authorises clients to perform protection and access operations on data, based on the client's identity and LDAP authentication credentials. • Verify that the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, and all communication between the TOE and other trusted IT products/remote users are initiated via trusted path/channels.	FIA_ATD.1.1, FIA_SOS.1.1 , FIA_UAU.2.1, FIA_UAU.5.1, FIA_UID.2.1, FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FPT_STM.1.1, FTA_SSL.4, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3

75 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

76 The evaluators performed vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and

an analysis of guidance documentation, functional specification, and TOE design and security architecture description.

77 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

78 The penetration tests focused on:

a) Port Scan

b) General Vulnerability Scan

c) Common Web Vulnerability Scan

d) Cookie Injection/ Broken Authentication

e) Input and Data Validation

f) Weak Cipher Strength

79 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a basic attack potential. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

80 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 with Augmented ALC_FLR.1 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

81 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Micro Focus Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10 performed by BAE Systems Applied Intelligence MySEF.

82 BAE Systems Applied Intelligence MySEF found that Micro Focus Voltage SecureData Appliance (SDA) v6.4 and SecureData Simple API v5.10 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented ALC_FLR.1.

83 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

84 EAL 2 provides assurance by a full Security Target and analysis of the SFRs in that Security Target (Ref [6]), using functional and interface specifications, guidance documentation and a basic description of the design and architecture of the TOE, to understand the security behaviours of the TOE.

85 The analysis is supported by an independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a Basic attack potential.

86 EAL 2 also provides assurance through use of a configuration management system, evidence of secure delivery procedures and basic flaw remediation (ALC_FLR.1).

3.2 Recommendation

87 The following recommendations are made:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) Potential purchasers of the TOE should consider the use of a CA signed certificate, as opposed to a self-signed certificate to fully secure access to the TOE environment.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1d, CyberSecurity Malaysia, February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, February 2016.

[6] Voltage SecureData Appliance and SecureData Simple API Security Target, Version 1.0, 1 November 2017

[7] EAU000426.06-S042-ETR 1.0, Evaluation Technical Report, Version 1.0, 29 November 2017

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target

Acronym	Expanded Term
TOE	Target of Evaluation
AES	Advanced Encryption Standard
API	Application Programming Interface
FPE	Format Preserving Encryption—an encryption method that encrypts data so that the cipher text has the same length and character set as the input data
HSM	Hardware Security Module—a physical computing device that manages and safeguards cryptographic keys and may support other cryptographic operations
IBE	Identity-Based Encryption—an asymmetric encryption algorithm that encrypts data without preserving its length or character set
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
REST	Representational state transfer—a software architecture for distributed systems, including RESTful API web services
SOAP	Simple Object Access Protocol—a protocol specification for exchanging structured information in the implementation of web services in computer networks.
SSL	Secure Sockets Layer

A.2.2 Glossary of Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.

Term	Definition and Source
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---