MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

C104 Certification Report

Verizon UniCERT v5.4.1

File name: ISCB-3-RPT-C104-CR-V1a
Version: V1a
Date of document: 15 July 2019
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)

T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Securing Our Cyberspace

C104 Certification Report

Verizon UniCERT v5.4.1

15 July 2019

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 Fax: +603 8008 7000
http://www.cybersecurity.my

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Malaysia

Registered in Malaysia – Company 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 15 July 2019, 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).

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

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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	3 July 2019	All	Initial draft
V1	8 July 2019	All	Change identifier and date release
V1a	15 July 2019	All	Additional updates on scheme policy according to Committee's comment

Executive Summary

The Target of Evaluation (TOE) is a software product which provides all the (PKI-specific) functionality needed to implement a Public Key Infrastructure (PKI) system.

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 with ALC_FLR.2. 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 according to the ISCB Product Certification Schemes Policy (Ref [4]).

The evaluation was performed by Securelytics SEF and the evaluation was completed on 5 July 2019.

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 Verizon UniCERT v5.4.1 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.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Verizon UniCERT is a software product which provides all the (PKI-sepcific) functionality needed to implement a Public Key Infrastructure (PKI) System. The primary function of a PKI system is to issue and manage digital certificates that allow other IT systems to verify the identity of the holder. UniCERT provides all the functionality needed to implement a PKI system, essentially a system that provides certificate registration, PKI management, a Certification Authority and certificate lifecycle management functions. The TOE can then be used to manage all the keys necessary for a system requiring security for end users, such as secure messaging system, or secure use of Web browsers. UniCERT provides the ability to set up a centralised or distributed PKI for organisations of any size.

2 The core components of the TOE are:

- **Certification Authority (CA) core component.** The CA is responsible for the generation and issuance (i.e. publication or distribution) of certificates and certificate revocation lists, and for the overall management of certificates and the PKI in general.
- **Registration Authority (RA) core component.** The RA is responsible for gathering registration information and revocation requests, authorising requests and handling renewals. The control over the functions the Registration Authority components are allowed to perform is provided by the Certification Authority Operator component.

3 In addition, the TOE may be configured with certain optional “advanced components” (other Verizon products); however, only two of these components may form part of the TOE:

- **The Key Archiver (KAS).** The KAS provides a facility to archive and retrieve private keys.
- **The Autoenroll Solution.** This component supports the automatic registration, generation, and distribution of certificates for use with computers in a Microsoft Windows domain.

4 Although the TOE provides all the PKI-specific functionality needed to implement a PKI system must be hosted on a hardware platform and must also include a Windows or

Linux operating system, such a system must be hosted on a hardware platform and must also include a Windows or Linux operating system, a database management system (Oracle), a

1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C104
TOE Name	Verizon UniCERT
TOE Version	v5.4.1
Security Target Title	Verizon UniCERT 5.4.1 Security Target
Security Target Version	v1.2
Security Target Date	1 July 2019
Assurance Level	Evaluation Assurance Level 2 Augmented with ALC_FLR.2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 2 Augmented with ALC_FLR.2
Sponsor	Teron Labs Pty Ltd
Developer	Verizon Australia Pty Ltd
Evaluation Facility	Securelytics SEF

1.3 Security Policy

6 There is no organisational security policy defined regarding the use of TOE.

1.4 TOE Architecture

7 The TOE includes both physical and logical boundaries which are described in Section 1.6 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

8 The TOE consists of the UniCERT core components (and their sub-components), the "advanced" component (and their sub-components), the utilities that are identified in the Security Target (Ref [6]).

Table 2: UniCERT Core Components

Standard cryptographic methods	The TOE provides capabilities for the generation, destruction, export, splitting and updating of cryptographic keys associated with the PKI system, TOE components, and TOE users based on standardized methods. Its implements standard digital signature methods to: • allow the content of certificates and CRLs to be verifiable and to prevent forgery and tampering • protect the integrity of data when at rest and when in transit between components of the TOE • protect the integrity of messages transmitted between components of the TOE (which may o may not be hosted on different platform)
Certificate lifecycle management	The TOE provides the capability to register entities for digital certificates through a range of methods, protocols and interface in accordance with operational policies defined for the TOE including email clients, windows clients, simple certificate enrolment protocol (SCEP), and web browser. The TOE provides an automated means for end users of a Microsoft Windows domain both human users and server components, such as domain controllers) to request certificates via the Autoenroller and RA component of the TOE. The TOE also provides the capability to securely generate or

	renew digital certificates, in accordance with pre-defined operational policies, via Certification Authorities, for its own use and for distribution to entities that include users, applications and devices.
Integration with hardware security modules	The TOE may also be securely integrated with dedicated HSM devices and smartcards that are PKCS#11 compliant devices. These devices can be used for the delivery of cryptographic services to the TOE and for securing of private keys related to the TOE components as required by the end user of the PKI system.
Key archival	The TOE provides a secure key repository and retrieval capability for end users' private encryption keys that enables end user to recover a key at a later date should the user's copy of the key become corrupt or lost. It also enables an organisation to recover encrypted data if a key/certificate owner leaves the company unexpectedly.
PKI management	The TOE provides a range of functions and utilities for secure management of the TOE and establishing the public key infrastructure implemented by the TOE as a hierarchy of Certification Authorities, Registration Authorities and other TOE components as required.
Security Audit	The TOE provides automated auditing facilities that include extensive capabilities for protecting, querying and archiving of audit records. Audit records are digitally signed when they are created (so unauthorised modifications can be detected) and written to the database associated with the component that generated the audit event.

1.4.2 Physical Boundaries

9 The TOE is a complex and flexible software product, and is comprised of several components, sub-components and utilities for the implementation of a public key infrastructure system. The components are described in details in Section 1.6 of the Security Target (Ref [6]).

Table 3: TOE Components, sub-components and utilities

Certification Authority (CA)	The TOE CA core component is the nucleus of the PKI system. It consists of the following sub-components such as: • **CA** (i.e. the main CA server), which generates certificates and CRLs; • **CA Operator** (CAO), which provides a GUI for authorized users to manage the PKI system in general; • **Publisher**, which distributes and publishes certificates and CRLs, using a variety of distribution methods and directory formats; and • **Certificate Status Server** (CSS), which responds to Online Certificate Status Protocol (OCSP) requests from other TOE components by providing real time certificate status information.
Registration Authority (RA)	The TOE RA core component provides a registration portal for the PKI system, and an interface to the CA component. It receives, verifies and forwards requests to the CA[1] and sends back the CA's response. It consists of the following sub components: • **RA** (i.e. the main RA server), which essentially acts as a router, transferring information between the CA and other RA sub-components; • A number of **Web Registration Authorities Operators** (WebRAOs), each of which enables a WebRAO user to authorize certificate and revocation

	requests. A WebRAO consists of a servlets part, which resides on the operational environment, and a client application, which may be (and usually is) hosted on an external system; - A number of **protocol handlers** (Web Handler, Email Handler, SCEP Handler), which convert requests received from an external system (in a variety of formats) into a common internal format; - **RA eXchange** (RAX), which provides a communication link between the RA, protocol handlers and WebRAOs; and - **RA Event Viewer**, which provides a GUI for authorized users to access audit records produced by the RA sub-components.
Key Archiver	Key Archiver provides a facility to archive and retrieve private keys and consists of the following sub components: - **Key Archive Server (KAS)**, which securely archives - in a KAS database - private keys received via the RA and KAO components. - **Key Archive Operator (KAO)**, which provides a GUI for authorized users to manage the KAS.
Autoenroll solution	The Autoenroll solution supports the automatic registration, generation and distribution of certificates to be used with computers in a Microsoft Windows domain. It consists of the following sub components: - **Autoenroll Handler**, which is a protocol handler that handles Microsoft Autoenroll requests, but differs somewhat from other protocol handlers in that it may be hosted on an external system. Hence, it is not classed as an RA sub-component (but it does communicate with the RA eXchange); - **Autoenroll Publisher**, which functions in a similar

	manner to the CA Publisher sub-component, but - because it needs to be co-located with the Autoenroll Handler - may be hosted on an external system. Hence, the CA communicates with the Autoenroll Handler (via the RAX) rather than with the Autoenroll Publisher directly.
Support Utilities	The support utilities are in the scope of the evaluation. These utilities are: • **Database Wizard.** The Database Wizard is used when first installing the TOE in order to create the required Oracle tables (i.e. schemas), and to create the necessary database user accounts. • **Database Upgrade Utility**. The Database Upgrade Utility is used where the TOE requires new or changed (Oracle) database tables (i.e. schemas) to be in place. • **Key Generator**. The Key Generator utility allows a CAO user to generate keys for TOE sub-components that reside on a different platform from where the CAO is installed. • **Publisher Configuration Utility**. The Publisher Configuration utility (also referred to as the Publisher Configuration program) allows an administrator to configure the Publisher and Autoenroll Publisher components of the TOE. This allows for the publication of certificates, CRLs and ARLs to a repository (LDAP or OCSP responder) external to the TOE. • **Token Manager**. The Token Manager allows a TOE user to manage personal secure environment files (PSEs), PKCS#12 files, and PKCS#11 tokens, used in the PKI system. It is a stand-alone utility that enables the user to view the contents of these files and

	tokens. - **Service Manager**. The Service Manager utility provides an interface that allows a TOE user to start and stop those TOE sub-components that provide a TOE service. For example, the CA, CSS, RA and RA eXchange sub-components.

1.5 Clarification of Scope

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

11 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]).

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

1.6 Assumptions

13 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Environmental assumptions

14 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 4: Assumptions for the TOE environment

Assumption	Statements

Assumption	Statements
A.AUTH_DATA_DISPOSAL	Authentication data and associated privileges are properly disposed of and/or removed as appropriate when no longer required within the PKI system. This includes both removal (secure deletion) of data from the PKI system, and the revocation of certificates. (For example, if CAO users leave the organization that runs the PKI system, then their certificate should be revoked and their private key securely destroyed. Similarly, if it is suspected that a private key has been compromised, then the associated certificate should be promptly suspended or revoked.)
A.AUDIT_REVIEW	Authorized auditor(s) regularly review audit records produced by the TOE, respond promptly to any indication of an attempted or actual security breach, and ensure that audit records are regularly archived to prevent audit data storage exhaustion.
A.COMPETENT_USERS	All (human) TOE users and those users managing the operational environment are competent, either by training or experience, to manage, operate and use the PKI system, and to maintain the security and privacy of the data it handles.
A.TRUSTED_USERS	All (human) TOE users and those users managing the operational environment are trusted, as far as is reasonably possible, not to abuse the PKI system facilities that they are authorized to use; in particular, they are trusted to not install or execute malicious software within the PKI system.
A.SECURE_INSTALL	The (human) TOE users and those users managing the operational environment install, configure and maintain the PKI system securely, i.e. in accordance with all relevant guidance documentation.

Assumption	Statements
A.COMMS_PROTECTION	There is adequate logical and physical protection on the communication channels used by the TOE. The protection extends to the boundary of the PKI system, and includes the use of firewall(s) to prevent unauthorized access to the PKI system via a communication channel.
A.PHYSICAL_PROTECTION	The PKI system has adequate physical protection against, in particular, unauthorized physical access by potential attackers.
A.TIME_SOURCE	There is a trusted, accurate, and reliable time source within the PKI system that may be used to timestamp TOE audit records.
A.ACCOUNTABILITY	The PKI system is configured and operated such that individual administrators or users can be held accountable for their actions.
A.ROLE_SEPARATION	The PKI system is configured and operated such that any separation of roles (as recommended in guidance documentation) is maintained.
A.HSM	Any HSM that will be integrated with the TOE is PKCS#11 compliant and the following security features are suitably assured: • Cryptographic key management (generation/destruction); • Cryptographic operations (digital signature generation); • Identification, authentication and access control; • Physical protection; and • Secure data exchange between the TOE and the HSM.

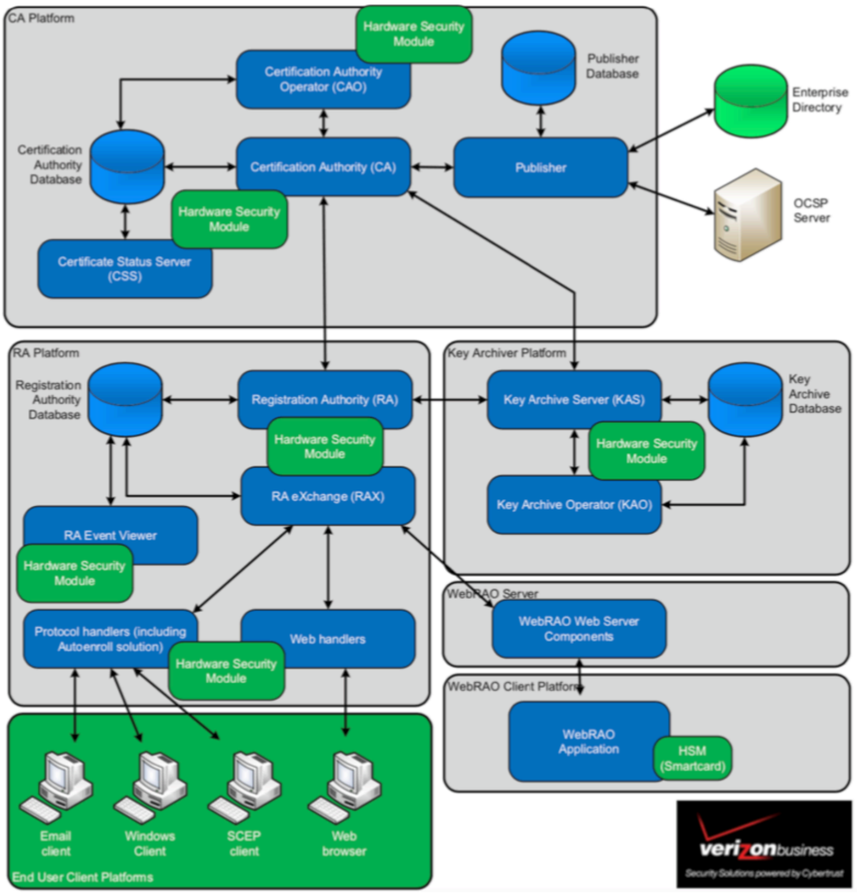
1.7 Evaluated Configuration

15 UniCERT may be deployed in a number of configurations consistent with the requirements identified in this Security Target (Ref [6]). Where the deployed environment satisfies the objectives stated in 4.2 in Security Target (Ref [6]). Valid configurations include the use of hardware security modules (HSM)s or smart cards and;

- Deployment of all TOE components on a single platform;
- Deployment of TOE components across multiple platforms with or without multiple components on a single platform; or
- Deployment of TOE components on virtual servers.

16 An example UniCERT deployment is illustrated in Figure 1 below. Those components shown in blue are included within the scope of the UniCERT evaluation, and those in green are external to the TOE.

Figure 1: Example UniCERT Deployment



17 The evaluator has verified that the TOE samples are provided in the above-described state. The combination of a correctly configured TOE and its operational environment (i.e. the non-TOE hardware and software) is referred to as "the PKI system" throughout Security Target (Ref [6]).

1.8 Delivery Procedures

18 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.

19 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 Ordering Procedures

20 Customer submits PO to Sales representative. Sales representative or Order Entry team complete the Sales Summary Report (SSR) and Sales Order Form (SOF). Both the SSR and SOF contain the following order detail such as company details, order type, product codes, product details etc.

21 **New Orders:** when all the necessary paperwork is approved and in place for the order, the order is uploaded to Verizon's online order system **One View International** (OVI) in the OECT9 queue by the order entry teams. The VIDM will review the full order detail within the attachments including the SSR/SOF, financial approvals, export screening(ESI) approval of all parties involved (which is essential pre shipment) requested through the ECS system.

22 **Customer software upgrade requests:** All software upgrade requests come through the Identity Account Management(IAM) team, who supply the full customer/end user and product detail to be shipped, along with the export screening(ESI) approval through the ECS system.

23 **Evaluation requests**: If the customer require an evaluation copy of the software (usually 90 days), the requester must complete an export screening approval through the ECS system and forward the approval mail to request the latest "evaluation license agreement" from the UniCERT product manager or VIDM, who can reject the request depending on the customer or end user involved. The evaluation agreement will be emailed to the customer direct or the requestor to forward to the customer. The customer confirms the products, signs and dates the agreement and returns the form by email to the UniCERT product manager and VIDM. If approved, the details are

entered onto the weekly "Sales, Distribution and Finance Spreadsheet" within the Evaluation tab section and shipped

1.8.2 Shipping the Software

24 When software is available for final release, it is burned onto a CDR or DVD, labelled with the version of the product and submitted to the VIDM along with the product release handover sheet signed by the Development and Product Managers.

25 The development department hand over the master copies to the VIDM, who will log them in the distribution new release log file held in the distribution room in Verizon Ireland. The following details are logged such as Product Name and Version, No. of CD's, date received, received by, date destroyed (if applicable).

26 The VIDM holds the key to a lockable fireproof cabinet where all master copies are stored within the distribution room, and also authorizes who has access controlled by swipe card to the distribution room within Verizon Ireland.

27 When an order is processed by distribution, a copy of the software is created on CDR or DVD, labelled and shipped to the customer via a courier within a tamper-evident bag with the following documentation such as Delivery Note, Original Export License (if required), Shipping (Commercial) Invoice and Courier Airway Bill.

28 The CD/DVD can only be written to once, therefore cannot be tampered with or overwritten. As an additional measure to ensure the content cannot be altered after the initial burning process, so the session is finalized once the CD/DVD has been copied.

29 The tamper-evident bag is to ensure any tampering to the packaging would be obvious to the customer before delivery. The tamper-evident bag has a unique identification number which is added to the Delivery note.

1.8.3 Tracking the Shipment

30 Distribution maintain separate weekly Sales, Distribution Spreadsheets for APAC, EMEA and US regions.

31 All shipments are tracked by entering the courier airway bill no. into the couriers tracking system which creates a tracking report with a detailed status of the shipment from pick up time to delivery and provides the Proof of Delivery(POD) at the Customer/End User location with the exact time and date of delivery and who signed for the shipment.

1.8.4 Invoicing the Customer

32 When the order is delivered, the VIDM triggers the order for billing to invoice the customer within the OVI order line items and attach the Delivery note and POD information.

1.9 Flaw Remediation Procedures

33 The evaluators 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 which would produce a description of each security flaw in terms of its nature and effects.

34 The evaluators examined the flaw remediation procedures and determined that the application of the procedures would identify the status of finding a correction to each security flaw and identify the corrective action for each security flaw.

35 The evaluators 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.

36 The evaluators examined the flaw remediation procedures and determined that it describes procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.

37 The evaluators examined the flaw remediation procedures and determined that the application of the procedures would help to ensure every reported flaw is corrected and that TOE users are issued remediation procedures for each security flaw.

38 The evaluators examined the flaw remediation procedures and determined that the application of the procedures would result in safeguards that the potential correction contains no adverse effects.

39 The evaluators examined the flaw remediation guidance and determined that the application of the procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

2 Evaluation

41 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 Augmented with ALC_FLR.2. The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

43 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

44 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.

2.1.2 Development

45 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

46 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

47 The evaluators examined the TOE security architecture description; they 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.

48 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

49 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

50 The evaluators confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

51 Testing at EAL 2 Augmented with ALC_FLR.2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

52 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, 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). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

53 At EAL 2 Augmented with ALC_FLR.2, 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.

54 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.

Table 5: Independent Functional Test

Test Suite	Description	Results
F001	To demonstrate the user creation process	Passed. Result as expected.
F002	To demonstrate the user configuration and rights setting process.	Passed. Result as expected.
F003	To create and populate authorisation groups	Passed. Result as expected.
F004	Verify that the TOE can generate cryptographic keys of various sizes (for use in protecting the LTSK) in accordance with AES and 3DES.	Passed. Result as expected.
F005	Verify that the TOE can generate cryptographic keys of various sizes in accordance with DSA, RSA and ECDSA.	Passed. Result as expected.
F006	Demonstrate the use of the key generator application.	Passed. Result as expected.
F007	To confirm that the password complexity requirements are enforced by the Token Manager.	Passed. Result as expected.
F008	To demonstrate that the TOE is able to generate a certificate signing request that is PKCS#10 compliant.	Passed. Result as expected.
F009	To demonstrate that information transmitted between TOE components is protected from unauthorised view or modification; protected through cryptographic controls.	Passed. Result as expected.

Test Suite	Description	Results
F010	Verify that authorised TOE users can authorise certificate requests.	Passed. Result as expected.
F011	To demonstrate the certificate revocation process	Passed. Result as expected.
F012	Demonstrate that key recovery can be performed.	Passed. Result as expected.
F013	To demonstrate that a revoked PKI component can no longer successfully perform actions within the PKI.	Passed. Result as expected.
F014	To demonstrate that an expired certificate may not be used to perform TOE operations.	Passed. Result as expected.
F015	Verify that a UniCERT CAO/KAO/RAA can open the (respective) event log, run a query and view a specific event log event.	Passed. Result as expected.
F016	Verify that a UniCERT CAO can validate the audit log.	Passed. Result as expected.
F017	Verify that a UniCERT CAO/KAO/RAA with the correct rights can archive the audit log.	Passed. Result as expected.
F018	Verify that a UniCERT CAO with insufficient rights is unable to view the audit log.	Passed. Result as expected.
F019	Demonstrate that the TOE generates audit logs for the various events performed by the TOE.	Passed. Result as expected.
F020	To demonstrate that users must be both identified and authenticated before being permitting any TSF mediated actions to be performed.	Passed. Result as expected.

Test Suite	Description	Results
F021	To demonstrate that a user attempting to authenticate to the TOE using key and certificate information not generated and authorised by the TOE will be unable to authenticate to the TOE and access any TOE mediated functionality.	Passed. Result as expected.
F022	To demonstrate that timestamps recorded by the TOE are the same as the system timestamps.	Passed. Result as expected.
F023	To demonstrate that only specific users can specify expiration times for certificates.	Passed. Result as expected.

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

2.1.4.3 Penetration testing

56 The evaluators performed a 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, TOE design, and security architecture description.

57 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack 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 (elapse time);

b) Specialist technical expertise required (specialised expertise);

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

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation

58 The penetration tests focused on:

a) Unencrypted communication channel;

b) DLL Hijacking;

c) Information Leakage in Files/folder;

d) Information Leakage in application Registry;

e) Information leak in memory;

f) Directory Traversal;

59 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in Section 4 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

60 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all the test conducted were PASSED as expected.

3 Result of the Evaluation

61 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 Verizon UniCERT v5.4.1 which is performed by Securelytics SEF.

62 Securelytics SEF found that Verizon UniCERT v5.4.1 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 Augmented with ALC_FLR.2.

63 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

64 EAL 2 Augmented with ALC_FLR.2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

65 The analysis is supported by 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 penetration attackers with a basic attack potential.

66 EAL 2 Augmented with ALC_FLR.2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

67 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) the potential consumer 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 in Security Target (Ref [6]).

b) The System Administrator should review the audit trail generated and exported by the TOE periodically.

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 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] ISCB Product Certification Schemes Policy (Product_SP), v1b, CyberSecurity Malaysia, March 2018.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1a, March 2018.

[6] Verizon UniCERT 5.4.1 Security Target, Version 1.2, 1 July 2019.

[7] Verizon UniCERT 5.4.1 Evaluation Technical Report, Version 1.1, 2 July 2019.

A.2 Terminology

A.2.1 Acronyms

Table 6: 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

A.2.2 Glossary of Terms

Table 7: 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.
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.

Term	Definition and Source
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 ---