MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C120 Certification Report

Verizon UniCERT v5.5.1

File name: ISCB-5-RPT-C120-CR-V1
Version: v1
Date of document: 19 May 2021
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

C120 Certification Report

Verizon UniCERT v5.5.1

19 May 2021

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

Document Authorisation

DOCUMENT TITLE:	C120 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C120-CR-V1
ISSUE:	v1
DATE:	19 May 2021
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. 201601006881(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 26 May 2021, 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	10 May 2021	All	Initial draft
v1	19 May 2021	All	Final Released

Executive Summary

The Target of Evaluation (TOE) is Verizon UniCERT v5.5.1. The TOE is a software product which provides all the (PKI-specific) 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. The TOE 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 a secure messaging system, or secure use of Web browsers. The TOE provides the ability to set up a centralized or a distributed PKI for organizations of any size.

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.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 (Ref [4]).

The evaluation was performed by Securelytics SEF and the evaluation was completed on 06 May 2021.

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 v5.5.1 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 Target of Evaluation (TOE) is Verizon UniCERT v5.5.1. The TOE is a software product which provides all the (PKI-specific) 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. The TOE 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 a secure messaging system, or secure use of Web browsers. The TOE provides the ability to set up a centralized or a distributed PKI for organizations of any size.

The TOE includes the following core components:

- **Certification Authority (CA) core component**. The CA core component is the CA Platform which 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 the RA Platform which is responsible for gathering registration information and revocation requests, authorizing requests, and handling renewals. It also includes the **WebRAO Servers** and **WebRAO Clients** which allow clients to interact with the RA remotely. The control over the functions the Registration Authority components are allowed to perform is provided by the Certification Authority Operator component.

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)** which allows archiving of the cryptographic keys.
- **The Autoenroll Solution**. This component supports the automatic registration, generation, and distribution of certificates for use with computers in a Microsoft Windows domain.

- Various **Utilities** to assist the operators of the TOE.

2 The TOE 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 (including certificates and CRLs) when at rest and when in transit between components of the TOE, allows TLS/SSL authentication of itself to the Enterprise Server to ensure that the Enterprise Server only accepts certificates published by a legitimate TOE and protect the integrity of messages transmitted between components of the TOE.

3 The TOE implements standard cryptographic methods for protecting the confidentiality of data and symmetric keys when at rest and when in transit between components of the TOE. The confidentiality of data is protected by symmetric cryptographic methods and the confidentiality of symmetric keys is protected by asymmetric cryptographic methods.

4 The TOE provides the capability to securely generate or renew digital certificates, in accordance with the operational policies defined for the TOE. The Certification Authorities perform this function for the TOE's own use and for distribution to entities that include users, applications and devices. Certificate generation binds the identity of an entity to a public key with a digital signature.

5 The TOE maintains the status of digital certificates issued by the TOE and allows entities to query the status of digital certificates using the Online Certificate Status Protocol (OCSP).

6 The The TOE provides the capability to suspend or revoke digital certificates where necessary, such as in response to suspected private key compromise. The TOE publishes revoked certificates on a Certificate Revocation List (CRL) in accordance with operational policy defined for the TOE.

7 While the TOE provides a range of standard cryptographic methods, 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 physically securing private keys related to the TOE components as required by the end user of the PKI system.

8 The TOE provides a secure key repository and retrieval capability for end users' private encryption keys; this enables an 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 organization to recover encrypted data if a key/certificate owner leaves the company unexpectedly.

9 The TOE provides a range of functions and utilities for secure management of the TOE, and for establishing the public key infrastructure implemented by the TOE.

10 The TOE provides automated auditing facilities that include extensive capabilities for protecting, querying, and archiving of audit records. The TOE supports assignment of authorized auditor roles for the management and review of audit logs generated by the TOE.

1.2 TOE Identification

11 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	C120
TOE Name	Verizon UniCERT
TOE Version	V5.5.1
Security Target Title	Verizon UniCERT Security Target
Security Target Version	V0.8
Security Target Date	01 April 2021
Assurance Level	Evaluation Assurance Level 2 Augmented 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 ALC_FLR.2
Sponsor	Teron Labs Unit 3, 10 Geils Court, Deakin, ACT 2600, Australia
Developer	Verizon Australia

Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Petaling Jaya, Selangor Darul Ehsan

1.3 Security Policy

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

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

14 The TOE consists of the UniCERT core components (and their sub-components), the “advanced” components (and their sub-components), the utilities and the security functions as defined.

- 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.
- Certificate lifecycle management: The TOE provides the capability to register entities for digital certificates through a range of methods, protocols and interfaces in accordance with operational policies defined for the TOE.
- Integration with hardware security modules and smartcards: While the TOE provides a range of standard cryptographic methods, the TOE may also be securely integrated with dedicated HSM devices and smartcards (another form of HSM) that are PKCS#11 [PCKS#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; this enables an 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 organization to recover encrypted data if a key/certificate owner

leaves the company unexpectedly. The Key Archive Server is under the control and management of the Key Archive Operator component of the TOE

- 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.
- Secure registration: The TOE implements optional LDAP over TLS/SSL authentication of the Published and the Enterprise Directory to ensure that the Enterprise Directory only accepts authentic certificates from the TOE. The administrator of the TOE may configure the authentication to take place.
- Security audit: The TOE provides automated auditing facilities that include extensive capabilities for protecting, querying, and archiving of audit records.

1.4.2 Physical Boundaries

15 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. These components are described in subsequent sections.

Table 2: TOE Components, sub-components and utilities

Certification Authority (CA)	The TOE CA core component is the CA Platform which is the nucleus of the PKI system. It consists of the following sub-components: • **CA** (i.e. the main CA server), which generates certificates and CRLs and stores them in the CA Database (**CA DB);** • **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 as well as stores them in the Publisher Database **(Publisher DB)**; 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 is the RA Platform which provides a registration portal for the PKI system, and an interface to the CA component. It receives, verifies and forwards requests to the CA 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 and stores the Registration related data to the Registry Authority Database (**RA DB)**; • 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 **Web Handlers** which are the routines managing the WebRAO interfaces, a **WebRAO Servlets** part, which resides on the operational environment, and a **WebRAO 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. It also provides mechanisms to recover a key at a later date, e.g. should (the original copy of) the key become corrupted, or should a cryptographic token on which (the original copy of) the key is stored be damaged or lost; and • **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 TOE implements utilities that support all the components and to reduce the likelihood of misconfiguration or errors by TOE users. 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. The Database Wizard is unable to modify data in the tables or the account privileges (but it can be used to change a database account's password). The Database Wizard does not implement any of the TOE's SFRs, and does not handle TSF data; it is provided solely to assist in the installation and setup of the TOE. • **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. The utility upgrades the existing schemas. • **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. The generated public key can be transferred to the CAO platform (using removable media) in order to create a certificate, which can then be transferred to the TOE sub-component's platform (again using removable media). This is required where a TOE sub-component stores its keys in PKCS#11 compliant hardware that is not accessible from the CAO platform. • **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

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

17 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]).

18 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

19 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

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

Table 3 : Assumptions for the TOE operational environment

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.

Assumption	Statements
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.
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);

Assumption	Statements
	· Identification, authentication and access control; · Physical protection; and · Secure data exchange between the TOE and the HSM.

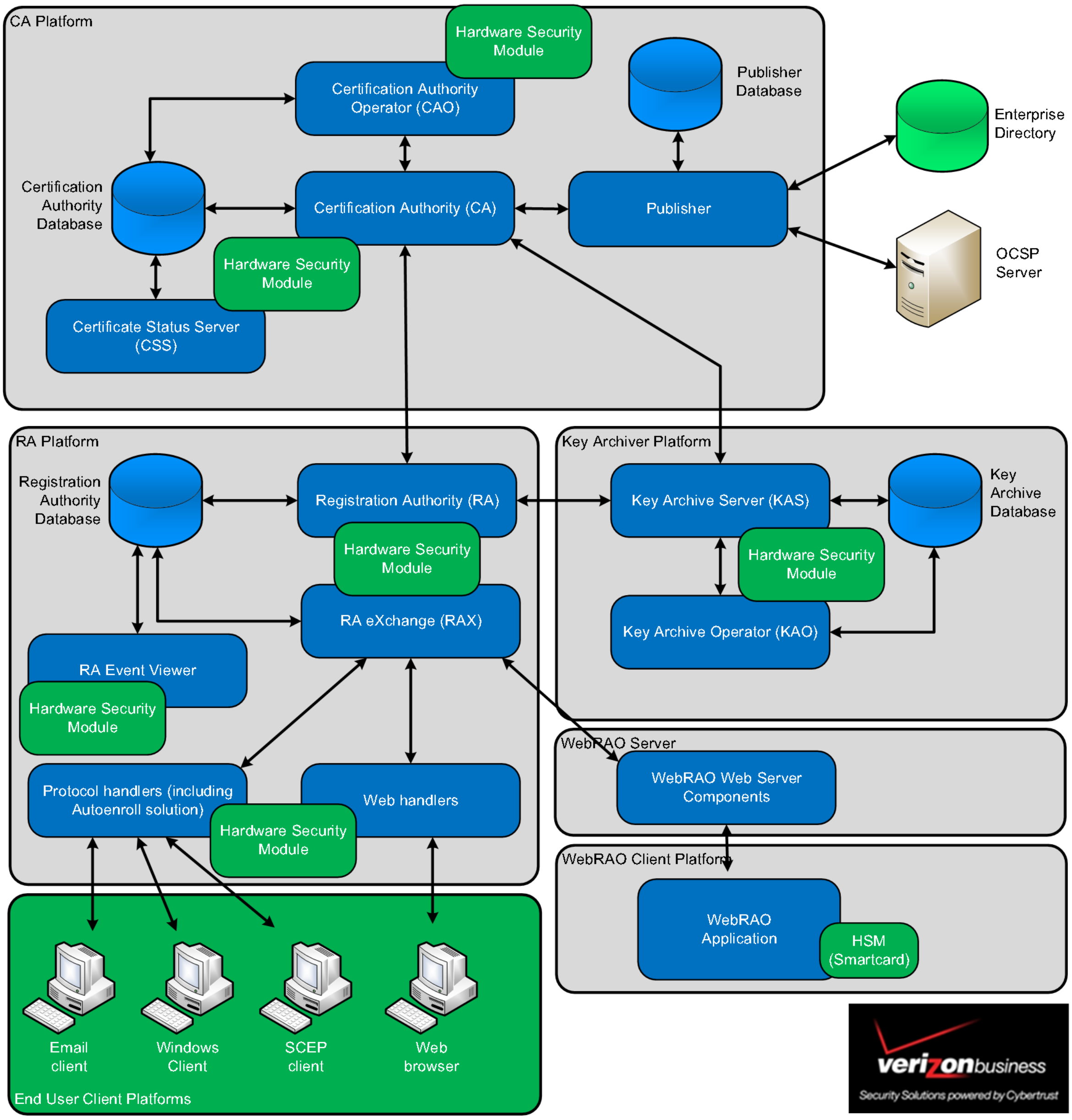
1.7 Evaluated Configuration

21 As 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.

22 An example UniCERT deployment is illustrated in **Error! Reference source not found.** below. Those components shown in blue are included within the scope of the UniCERT evaluation, and those in green (and the OCSP Server) are external to the TOE.

Figure 1: Example UniCERT deployment



23 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

24 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.

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

1.8.1 TOE Delivery Procedures

26 The TOE is delivered to the customer on a recordable compact discs (CDRs) that are delivered via mail in a tamper-evident bag with a delivery note attached to it. The tamper-evident bag is a DHL shipping bag with a unique ID. Once sealed, the bag can only be ripped to open which will ensure that the recipient will notice any attempted tampering. A tracking email is also sent by DHL to the customer. The tracking email includes information detailing the delivery and bag contents.

27 Upon receipt of the bag, the customer is required to check the tamper-evident bag to ensure that it has not been opened or otherwise tampered with, and to check that the ID of the tamper-evident bag (bag number) matches the information provided in both the delivery note and DHL's tracking email (sent directly to the customer) to ensure that the tamper-evident bag was not replaced with another one.

2 Evaluation

28 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. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

30 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.

31 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 Flaw Reporting Procedures

32 The evaluators have 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.

33 The evaluators have 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.

34 The evaluators have 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.

35 The evaluators have 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.

36 The evaluators have 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.

37 The evaluators have 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.

38 The evaluators have 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.

2.1.3 Development

39 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).

40 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.

41 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.

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

2.1.4 Guidance documents

43 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.

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

2.1.5 IT Product Testing

45 Testing at EAL 2 Augmented 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 Plan Report.

2.1.5.1 Assessment of Developer Tests

46 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.

2.1.5.2 Independent Functional Testing

47 At EAL 2 Augmented 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.

48 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 4 : Independent Functional Test

Test ID	Description	SFRs	Results
F001	To test that the TOE: · Generate cryptographic keys in accordance with a specified cryptographic key generation algorithm AES, 3DES, DSA, RSA, ECDSA · Enforce the [PKI access SFP] and allow the [a CAO User with any necessary permissions] to specify alternative initial values · Maintains user roles as stated in Table 20 of Annex C of ST · Maintains security attributes (role, assigned permissions, private key and associated passphrase to access the key, entity type certificate extension, X.509 certificate) · Capable of performing security management functions stated in Section 5.3.7.6 of ST	FCS_CKM.1, FMT_MSA.3, FMT_SMR.1, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FMT_SMF.1	Passed
F002	To test that the TOE: · Enforce the PKI access SFP to restrict the ability to query,	FMT_MSA.1, FMT_SMF.1, FDP_ACC.1, FDP_ACF.1	Passed

Test ID	Description	SFRs	Results
	modify, delete the security attributes (viewing and modifying the authorisations assigned to TOE users (including role, possible permissions, Assigned Permissions, X.509 Certificate) to a CAO User with any necessary permissions · Capable of performing security management functions stated in Section 5.3.7.6 of ST		
F003	To test that the TOE: · Capable of performing security management functions stated in Section 5.3.7.6 of ST	FMT_SMF.1, FDP_ACC.1, FDP_ACF.1	Passed
F004	To test that the TOE: · Enforce the PKI access SFP on the subjects, object and operations referenced in Annex C · Enforce the PKI access SFP to objects based on the following: • subjects as defined as a role referenced in Table 20 and Table 21 of Annex C with the following attributes:	FDP_ACC.1, FDP_ACF.1	Passed

Test ID	Description	SFRs	Results
	• Assigned Permissions • Private key and associated passphrase to access the key • X.509 Certificate • Objects and their associated attributes as referenced in Table 22 of Annex C of ST · Enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed		
F005	To test that the TOE: · Generate cryptographic keys in accordance with a specified cryptographic key generation algorithm AES, 3DES, DSA, RSA, ECDSA · Provide a mechanism to verify that secrets meet: • All passphrases must contain a minimum of eight characters. • Passphrases can contain non-ASCII (including foreign language) characters. • Passphrases consisting of all ASCII characters must contain at least one lowercase letter, one uppercase letter, one numerical digit, and one punctuation mark	FCS_CKM.1, FIA_SOS.1, FDP_ACC.1, FDP_ACF.1	Passed

Test ID	Description	SFRs	Results
F006	To test that the TOE: · Distribute cryptographic keys in accordance with a specified cryptographic key distribution method; PKCS#11, PKCS#12, PSE (Verizon proprietary) · Maintains security attributes (role, assigned permissions, private key and associated passphrase to access the key, entity type certificate extension, X.509 certificate) · Maintains user roles as stated in Table 20 of Annex C of ST · Capable of performing security management functions stated in Section 5.3.7.6 of ST	FCS_CKM.2, FMT_MSA.3, FMT_SMR.1, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FMT_SMF.1	Passed
F007	To test that the TOE: · Provide a mechanism to verify that secrets meet: • All passphrases must contain a minimum of eight characters. • Passphrases can contain non-ASCII (including foreign language) characters. • Passphrases consisting of all ASCII characters must contain at least one lowercase letter, one uppercase letter, one numerical digit, and one punctuation mark	FIA_SOS.1	Passed

Test ID	Description	SFRs	Results
F008	To test that the TOE able to generate a certificate signing request that is PKCS#10 compliant.	N/A	Passed
F009	To test that the TOE: · Perform RSA asymmetric encryption and decryption · Perform AES, 3DES symmetric encryption and decryption · Enforce the PKI messaging SFP to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE	FCS_COP.1/ asymmetric, FCS_COP.1/ symmetric, FDP_ITT.1, FPT_ITT.1/ all data, FPT_ITT.1/ private-secretkeys	Passed
F010	To test that the TOE: · Distribute cryptographic keys in accordance with a specified cryptographic key distribution method; PKCS#11, PKCS#12, PSE (Verizon proprietary)	FCS_CKM.2, FDP_ACC.1, FDP_ACF.1,	Passed

Test ID	Description	SFRs	Results
F011	To test that the TOE: · Enforce the PKI access SFP on the subjects, object and operations referenced in Annex C · Enforce the PKI access SFP to objects based on the following: • subjects as defined as a role referenced in Table 20 and Table 21 of Annex C with the following attributes: ○ Assigned Permissions ○ Private key and associated passphrase to access the key ○ X.509 Certificate ○ Objects and their associated attributes as referenced in Table 22 of Annex C of ST · Enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed	FDP_ACC.1, FDP_ACF.1	Passed
F012	To test that the TOE: · Perform cryptographic key archival and cryptographic key recovery in accordance with a specified cryptographic key access method [encryption using LTSK] · Capable of performing security management functions stated in Section 5.3.7.6 of ST	FCS_CKM.3, FDP_ACC.1, FDP_ACF.1, FMT_SMF.1	Passed

Test ID	Description	SFRs	Results
F013	To test that the TOE: · Capable of performing security management functions stated in Section 5.3.7.6 of ST · Enforce the PKI messaging SFP	FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FDP_ITT.3, FMT_SMF.1	Passed
F014	To test that the TOE: · Capable of performing security management functions stated in Section 5.3.7.6 of ST · Enforce the PKI messaging SFP · Restricts the capability to specify an expiration time for certificate validity to a CAO User or a WebRAO user (with any necessary permissions · Able to disallow the use of the relevant certificate after the expiration time for the indicated security attribute has passed. · Associate the following user security attributes with subjects acting on behalf of that user; Role, Assigned Permissions (as defined in Table 21 of Annex C), Entity type certificate extension, X.509 Certificate	FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FMT_SAE.1, FMT_SMF.1, FIA_USB.1	Passed

Test ID	Description	SFRs	Results
F015	To test that the TOE: · able to generate and record audit records · Provide the ability to perform searches, sorting and ordering of audit data based on queries as defined in the CAO documentation or RA Event Viewer documentation or Key Archive Operator documentation · Capable of performing security management functions stated in Section 5.3.7.6 of ST	FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FMT_SMF.1, FDP_ACC.1, FDP_ACF.1	Passed
F016	To test that the TOE: · Enforce the PKI access SFP on the subjects, object and operations referenced in Annex C · Enforce the PKI access SFP to objects based on the following: • subjects as defined as a role referenced in Table 20 and Table 21 of Annex C with the following attributes: ○ Assigned Permissions ○ Private key and associated passphrase to access the key ○ X.509 Certificate ○ Objects and their associated attributes as referenced in Table 22 of Annex C of ST	FDP_ACC.1, FDP_ACF.1	Passed

Test ID	Description	SFRs	Results
	· Enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed		
F017	To test that the TOE: · Provide the ability to perform searches, sorting and ordering of audit data based on queries as defined in the CAO documentation or RA Event Viewer documentation or Key Archive Operator documentation · Protect the stored audit records in the audit trail from unauthorized deletion. · Detect unauthorized modifications to the stored audit records in the audit trail. · Capable of performing security management functions stated in Section 5.3.7.6 of ST	FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FMT_SMF.1, FDP_ACC.1, FDP_ACF.1,	Passed
F018	To test that the TOE: · Prohibit all users read access to the audit records, except those users that have been granted explicit read-access. · Associate the following user security attributes with subjects acting on behalf of that user; Role, Assigned Permissions (as defined in Table 21 of Annex C), Entity type certificate extension, X.509 Certificate	FAU_SAR.2, FIA_USB.1	Passed

Test ID	Description	SFRs	Results
F019	To test that the TOE: · Able to generate and record audit records · Provide CAO Audit Manager, CAO Auditor, RA Audit Manager, RA Auditor, KAO Audit Manager, KAO Auditor with the capability to read all audit records from the audit records. · Provide the audit records in a manner suitable for the user to interpret the information.	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FDP_ACC.1, FDP_ACF.1	Passed
F020	To test that the TOE: · Require each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user · Restricts the ability to change default, query, modify, delete, clear the viewing and modifying the TOE configuration and TOE component configurations and registration policies to CAO User with any necessary permissions (except for audit records), CAO Audit Manager (for CA audit records), RA Audit Manager (for RA audit records) and KAO Audit Manager (for KAS audit records)].	FIA_UAU.2, FIA_UID.2, FMT_MTD.1 FMT_SMF.1, FIA_USB.1	Passed

Test ID	Description	SFRs	Results
	· Capable of performing security management functions stated in Section 5.3.7.6 of ST · Associate the following user security attributes with subjects acting on behalf of that user;Role, Assigned Permissions (as defined in Table 21 of Annex C), Entity type certificate extension, X.509 Certificate		
F021	To test that the TOE: · Provides a capability to generate evidence that can be used as a guarantee of the validity of each certificate and CRL generated by the TSF · Provides the ability to verify evidence of the validity of the indicated information and the identity of the user that generated that evidence. · Enforce the generation of evidence of origin for transmitted BRSP messages from protocol handlers except the WebHandler, Registration request messages, renewal request messages, revocation request messages,	FDP_ACC.1, FDP_ACF.1, FDP_DAU.2, FCO_NRO.2, FDP_ITT.1, FIA_USB.1, FCS_COP.1/ digitalsign, FCS_COP.1/ hash	Passed

Test ID	Description	SFRs	Results
	BRSP messages from all protocol handlers; Authorization request messages, Key recovery request messages, BRSP messages between the WebRAO and the RAX, CMP messages between; The CA and the RA, The RA and the KAS, The CA and the KAS at all times. · enforce the PKI messaging SFP · perform digital signatur creation and verification		
F022 F023	To test that the timestamps recorded by the TOE are the same as the system timestamps.	FPT_STM.1	Passed

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

2.1.5.3 Vulnerability Analysis

50 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, security architecture description, implementation representation and as well as available public information.

51 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 (elapsed 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 equipment required for exploitation.

2.1.5.4 Vulnerability testing

52 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 and database

f) Input Validation and Directory Traversal

g) Binary Manipulation

53 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 the Security Target (Ref [6]).

2.1.5.5 Testing Results

54 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

55 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 v5.5.1 which is performed by Securelytics SEF.

56 Securelytics SEF found that Verizon UniCERT v5.5.1 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 ALC_FLR.2.

57 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

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

59 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.

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

3.2 Recommendation

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

a) The users should make themselves familiar with the developer guidance provided with the TOE, pay attention to all security warnings as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

b) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.

c) System Auditor 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] MyCC Scheme Requirement (MYCC_REQ), v1, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2, December 2019.

[6] Verizon UniCERT Security Target, Version 0.8, 01 April 2021.

[7] Evaluation Technical Report – Verizon UniCERT, Version 1.0, 06 May 2021.

A.2 Terminology

A.2.1 Acronyms

Table 5 : 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

Acronym	Expanded Term
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6 : 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

Term	Definition and Source
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 ---