C072 Certification Report

CENTAGATE v3.0.10-build13

File name: ISCB-3-RPT-C072-CR-v1
Version: v1
Date of document: 6 June 2017
Document classification: PUBLIC

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

CyberSecurity Malaysia
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

C072 Certification Report
CENTAGATE v3.0.10-build13

6 June 2017

ISCB Department

CyberSecurity Malaysia

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

Document Authorisation

DOCUMENT TITLE:	C072 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C072-CR-v1
ISSUE:	v1
DATE:	6 June 2017

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

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

Disclaimer

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

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	18 May 2017	All	Initial draft of the certification report
v1	30 May 2017	All	Minor changes to make final.
v1	6 June 2017	iv	Changes to the evaluated and certified date

Executive Summary

This report documents the assessment of the Malaysian Common Criteria Certification Body (MyCB) team against the technical evaluation performed by licensed CyberSecurity Malaysia MySEF (Malaysian Security Evaluation Facility) on CENTAGATE v3.0.10-build13 and its components as defined in Security Target ([6]), EAL4+ ALC_FLR.2, developed and sponsored by SecureMetric Technology Sdn. Bhd.

The kick-off meeting was formally commenced on 16th February 2016 and the technical evaluation exercise was completed on 17th May 2017 with the submission of final Evaluation Technical Report.

CENTAGATE is an enterprise class authentication solution built on JEE technology, that enforce secure authentication for protected resources such as internal web applications. It operates through web interfaces and has the functionality that enables three-factor of authentications and risk-based scoring engine through accessibility of single sign-on (SSO). It consists of Web Application Server and Mobile Applications that supports Android and iOS platform.

The scope of evaluation covers major security features such as Security audit, User data protection, Identification and authentication, Security management, TOE access and Cryptographic key management.

The scope of the evaluation is defined by the Security Target ([6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security function 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 4 (EAL4) 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]). This Certification Report applies only to the specific version of the TOE as evaluated.

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 www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that CENTAGATE meet 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 CENTAGATE (also known as the TOE) is an enterprise class authentication solution built on JEE technology, allowing enterprise users to securely perform authentication before login to the application.

2 It enforces secure authentication for protected resources such as internal web applications and it also operates through web interfaces and has the functionality that enables three-factor of authentications and risk-based scoring engine through accessibility of single-on (SSO).

3 The risk-based scoring engine (also known as Hybrid Risk Scoring Engine) will calculate each user login attempt to access the protected resources based on defined security attributes and behaviour of each previous user login attempts.

4 The TOE consists of two major components in its operational environment, stated as the following:

a) TOE Web Application Server, which is the CENTAGATE v3.0.10-build13; and

b) TOE Mobile Applications, reside on these two platforms: Android (v1.0.10-build1) and iOS (v1.04-build1)

5 Overall, this security feature detects possible fraud or digital attacks and provides defend against common authentication attacks with a strong authentication feature supported by CENTAGATE Advance Mobile components (running on Android application or iOS application).

6 The TOE security functions defined as part of the TOE scope covered in the evaluation are stated as below:

a) Security Token Provision;

b) Mobile Protection;

c) Mobile PKI;

d) Hybrid Risk Scoring Engine (Rule-based and Case-based);

e) Cryptographic Module;

f) Key Management System;

g) Authentication Module;

h) Web Administration Module; and

i) Mobile Management Module.

1.2 TOE Identification

7 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	C072
TOE Name	CENTAGATE, consist of Web Application Server and Mobile Applications.
TOE Version	Web Application Server: CENTAGATE v3.0.10-build13; and Mobile Applications: Android (v1.0.10-build1) and iOS (v1.0.4-build1)
Security Target Title	Security Target for CENTAGATE
Security Target Version	3.0
Security Target Date	8 May 2017
Assurance Level	EAL4+ Augmented with ALC_FLR.2
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3]).
Protection Profile Conformance	None.
Common Criteria Conformance	CC Part 2 Conformant. CC Part 3 Conformant. Package conformant to EAL4+ Augmented with ALC_FLR.2
Sponsor and Developer	SecureMetric Technology Sdn. Bhd.
Evaluation Facility	CyberSecurity Malaysia MySEF (Malaysian Security Evaluation Facility).

1.3 Security Policy

8 Hybrid Risk Scoring Engine (Rule-based) as part of the Security Policies can be configured by the TOE Administrators (CENTAGATE Administrators and/or CENTAGATE Company Administrators) to suit the TOE operational environment, based on the security attributes defined in the configuration security policies at such: Browser Type, Operating System Type, Time, IP Address and Geo-location. The TOE Administrators can configure the Case-based Security Policies as part of the Hybrid Risk Scoring Engine, which will provide black list or white list access to the TOE and protected resources (Applications registered in the TOE, App Tab) by comparing the IP Address and/or Country of the users. The audit and alerts services ensure that all the security events that were recorded by the TOE and summary of audit reports are generated upon request in reporting the overall information.

1.4 TOE Architecture

9 The TOE components as described in scope consist of Web based Application System and Mobile Applications (Android and iOS). The underlying components of the web based application system are Hybrid Risk Scoring Engine, Cryptographic Module, Key Management System, Authentication Module, Web Administration Module and Mobility Management Module while Mobile Applications consist of Security Token Provision, Mobile Protection and Mobile PKI as the underlying components as described in the scope boundaries.

10 The TOE includes both logical and physical boundaries which are described in Section 1.3 of the Security Target (Ref[6]).

1.4.1 Logical Boundaries

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

a) Security Token Provision (SFR Mapped: Cryptographic Support)

b) Mobile Protection (SFR Mapped: Cryptographic Support)

c) Mobile PKI (SFR Mapped: Identification and Authentication, Security Management, User Data Protection, Cryptographic Support)

d) Hybrid Risk Scoring Engine (SFR Mapped: Security Audit, Identification and Authentication, Security Management, TOE Access, User Data Protection)

e) Cryptographic Module (SFR Mapped: Security Management, User Data Protection, Cryptographic Support)

f) Key Management System (SFR Mapped: Security Management, User Data Protection, Cryptographic Support)

g) Authentication Module (SFR Mapped: Security Audit, Identification and Authentication, Security Management, User Data Protection)

h) Web Administration Module (SFR Mapped: Security Audit, Identification and Authentication, Security Management, TOE Access, User Data Protection)

i) Mobility Management Module (SFR Mapped: Security Management, User Data Protection, Cryptographic Support)

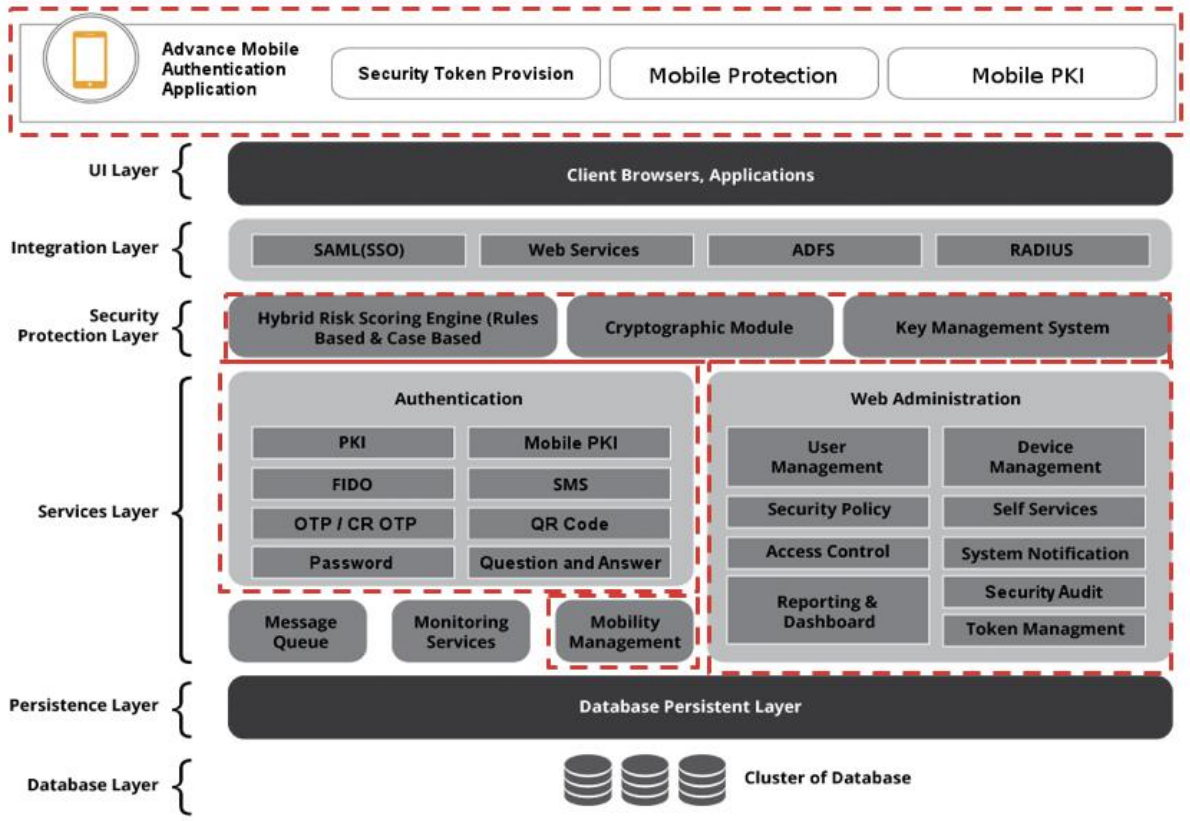

Figure 1: TOE diagram shows the Logical Boundaries of the TOE

TOE Boundary

12 Additionally, all underlying hardware and operating system running to support the TOE operational environment is not part of the scope of the TOE.

1.4.2 Physical Boundaries

13 The web application server consists of Web Application and Core Engine. These two main components work together to allow TOE authentication process flow to be executed via any relevant Internet Browser where the hybrid Risk Scoring Engine module will be performing risk calculation.

14 To enforce any methods of authentications available, the registration process is required to register all the relevant information and components such as the credentials of user linked to Advance Mobile Authentication Application.

15 Note that all operations of the TOE inclusive of its installation process, management of the TOE and handling of the TOE shall be elaborate further in the Guidance documentations.

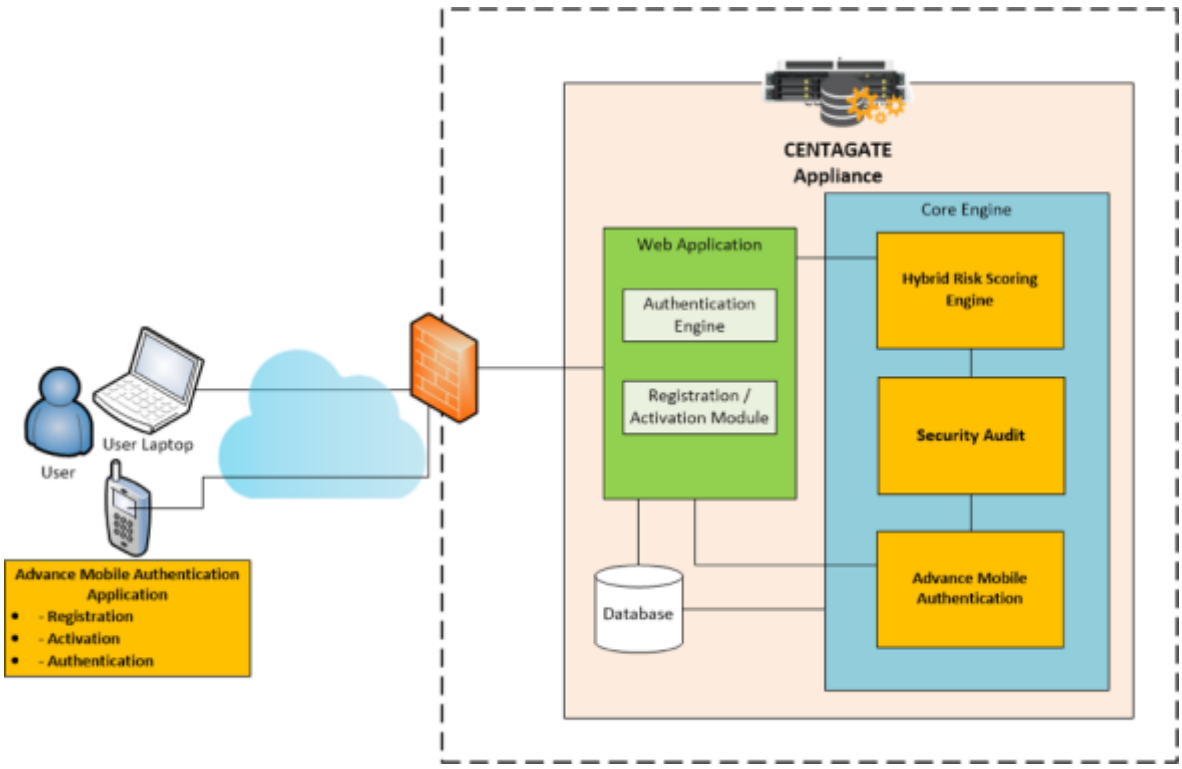

Figure 2: Physical Boundaries of the TOE

1.5 Clarification of Scope

16 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref[6]). The TOE which consists of two main components, where web application server as the authentication processor and Advance Mobile Authentication Application as the registration, activation and authentication module itself.

17 Note that FIDO and OTP Hardware Token is not part of the scope of the TOE. Offline registration methods only allow binding of OTP Hardware token, where this is out of the evaluation. SMS service to register the device is also out of scope.

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

1.6 Assumptions

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

1.6.1 Usage assumptions

20 The following is the assumption for the TOE usage:

a) The TOE Administrators and CENTAGATE users are non-hostile and trusted to perform all their duties in a competent manner.

b) Competent TOE Administrators will be assigned to manage the TOE and the security of the information it contains.

c) It is assumed that all codes used by the TOE for signing which are trusted only will be executed by the TOE.

d) The TOE Administrators shall ensure the OS Backend Server have been hardened to counter the perceived threats.

e) Only authorized individuals assigned by the organization will be given access to the TOE.

1.6.2 Environment assumptions

21 The following is the assumptions of the TOE environment:

a) The environment setup shall provide reliable time stamp to the TOE.

b) The environment will provide a mail server to facilitate alerts for TOE.

c) The environment is configured to block all traffic to the Identity access management server (TOE) except for traffic required to perform security functionality.

d) The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through the TOE.

e) The protection shall ensure the TOE will be protected from unauthorized physical modification and access.

f) Data collected and produced by the TOE shall be protected from unauthorized deletion or modification.

1.7 Evaluated Configuration

22 The TOE shall be configured according to the Preparative Guidance.

23 The TOE is delivered as an appliance by the developer, and the administrator must then make the following configuration changes:

a) Ensure that the TOE has an appropriate password for each administrator account;

b) Ensure that TOE management is performed from a secure network on its own physical interface;

c) Ensure that access to the TOE management network is restricted;

d) The usage of mobile devices that installed with the TOE mobile application shall be managed accordingly with protection are being applied such as: equipped with antivirus, operating system is not being rooted/jailbreak (Android/iOS), and PIN code uses by the TOE Mobile App User shall be random (not in numbering order, e.g. 123456); and

e) Deploy a trusted VPN to ensure that traffic to the TOE management network cannot be intercepted in transit.

24 The detailed requirement of evaluated Firmware/Hardware/Software for Web Application Server and mobile application can be referred in Security Target (Ref[6]) in Section 1.2.1 Table 4 and Table 5.

1.8 Delivery Procedures

25 The delivery procedure for the TOE is as follows:

a) The TOE shall be prepared by the developer at developers site before sending or delivering to the client/consumer site.

b) Developer shall prepare the Administrative and User Guidance document for TOE.

c) Labelling of the TOE are visible and validate through physical checks by the client during delivery of the TOE.

d) User Acceptance Test (UAT) shall be perform accordingly based on the outline drafted by the client, upon client requisition.

1.9 Documentation

26 List the documentation and description provided by the developer that the user can use as guidance to installation:

a) Operational User Guidance Introduction;

b) CENTAGATE Administrator Guide;

c) Rules-Based Policy User Guide;

d) CENTAGATE Company Administrative Guide;

e) CENTAGATE End User Guide;

f) CENTAGATE Mobile Applications User Guide

g) CENTAGATE API;

h) Preparative Procedure;

i) CENTAGATE Web Administration Console (Installation Guide);

j) CENTAGATE Mobile Application Installation Guide;

k) Appliance Installation Guide;

l) CENTAGATE Box Pre-Installation Checklist; and

2 Evaluation

27 The evaluation was conducted in accordance with the requirement of the Common Criteria, Version 3.1 Revision 4 (Ref[2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 4 (Ref[3]). The evaluation was conducted at Evaluation Assurance Level 4 (EAL4) with augmented ALC_FLR.2. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref[4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref[5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

29 An analysis of the CENTAGATE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items.

30 It is evaluated that the implemented configuration management system can control changes to those items that have been placed under configuration management system. The developer's configuration management system was also observed during the site visit, and it was found security flaws under configuration management ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution. This is evaluated to be consistent with the provided evidence.

31 During the site visit the evaluators examined the development security documentation and determined that it detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the CENTAGATE design and implementation. The evaluators confirmed that the developer used a documented life-cycle model which provides necessary control over the development and maintenance of the TOE by using the procedures, tools and techniques described by the life-cycle model.

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

2.1.2 Development

33 The evaluators analysed the CENTAGATE functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and modules. The design described the TOE subsystems to sufficiently determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing modules and enough information about the SFR-

supporting and SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented.

34 The evaluators analysed the TOE security architectural description and determined that the delivery and installation process was secure and the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

2.1.3 Guidance documents

35 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.

2.1.4 IT Product Testing

36 Testing at EAL4 augmented with ALC_FLR.2 consists of assessing developer tests, performing independent function test, and performing penetration tests. The CENTAGATE testing was conducted at CyberSecurity Malaysia MySEF and at the developer's site where it was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

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

38 Thirty-nine (39) test case scenarios were developed by the developer to ensure that each of the security functions were tested. Whilst, for each security functions defined as part of the scope of TOE has a primary function as its focus; they were all tested in the approaches of combination of the security functions or as individual components of its own.

39 The evaluators analysed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the implementation representation, functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

40 Independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a sample of the developer's test plan, and creating test cases that augmented the developer tests.

41 In addition, the evaluators developed four group of test cases as the independent tests to verify the behaviour of TOE based on the understanding of evaluators towards the TOE security functions and components, in which, meeting the requirements of the consumer products or a component of IT systems. Due to large scope of the TOE, various scenarios have been developed to ensure the whole scope has been tested. The developer's test has been used to develop different test case scenarios to test the TOE security functions in different ways.

42 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Four independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

DESCRIPTION	TOE SECURITY FUNCTIONAL	TSFI	RESULT
Examined the process of the TOE control access and privilege for each user of the TOE.	Advance Mobile Authentication Application	**Internal TSFI:** Mobile Token Provisioning Mobile Protection Mobile PKI Hybrid Risk Scoring Engine Authentication – PKI Authentication – FIDO Authentication – SMS Authentication – OTP/CR OTP Authentication – QR Code Authentication – Password Authentication – Question and Answer Cryptographic Key Management Subsystem Web Administration Subsystem Mobility Management **External TSFI:** Between CENTAGATE Administrator and TOE server Between CENTAGATE Company Administrator & TOE server	Passed
Examined the process of the TOE managed the TSF as well as managing the user of the TOE.	Web Administration		Passed
Examined the process of the TOE validate and verify each TOE user's accessibility to the protected resources managed by the TOE.	Hybrid Risk Scoring Engine		Passed
Examined the process of the TOE managed in the cryptographic processes in the TSF	Cryptographic Key Management		Passed
Examined the processes of the TOE managed the authentication	Authentication		Passed

process of the TOE users		Between CENTAGATE end user and TOE server Between TOE Users and TOE Mobile App	
Examined the processes of the TOE managed the TOE User mobile accessibility	Mobility Management		Passed

2.1.4.3 Penetration Testing

43 The evaluators performed vulnerability assessment and penetration tests based on an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description, implementation representation as well as available public information. The evaluators used these tests results to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced Basic attack potential. The following factors have been taken into consideration during the penetration tests:

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

b) Specialist technical expertise required (specialist expertise);

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

d) Window of opportunity; and

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

44 The penetration testing did not uncover any exploitable vulnerability in the anticipated operating environment. However, the results of the penetration testing note that a number of additional residual vulnerabilities exist as per stated in section 4.3.6 of Evaluation Technical Report (Ref[7]) that are dependent on an attacker effort, time, skill/knowledge, and focused tools/exploits use to gather the TOE and environment configuration information. Therefore, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

45 The penetration tests focused on:

a) Scanning;

b) XSS;

c) Sniffing;

d) Injection;

e) Cookies Manipulation;

f) Un-Validated Redirects and Forwards; and

g) Mobility Security Assessment through Static and Dynamic Analysis.

2.1.4.4 Testing Results

46 Tests conducted for the CENTAGATE produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

47 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing Enhanced Basic attack potential value between 14 to 19.

3 Result of the Evaluation

48 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 CENTAGATE v3.0.10-build13 performed by CyberSecurity Malaysia MySEF.

49 CyberSecurity Malaysia MySEF found that CENTAGATE v3.0.10-build13 upholds the claims made in the Security Target (Ref[6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL4+ ALC_FLR.2.

50 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. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

51 EAL4 provides assurance by a full Security Target (ST) and an analysis of the security functions in the ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation to understand the security behaviour.

52 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis demonstrating resistance to penetration attackers with an Enhance Basic attack potential.

53 EAL4 also provides assurance though the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

3.2 Recommendation

54 Opinions and interpretations expressed herein are outside the scope of SAMM accreditation.

55 This section list the evaluator recommendations that should be considered in the deployment of the TOE:

a) Consumer/Client that have intention of purchasing the TOE are recommended to keep on updating, maintaining, backing up configuration, logs and related data/files of TOE and performing checks on the TOE regularly to maintain its secure operational environment. A strict adherence on documentations and procedures provided by developer to consumer/client are highly recommended.

b) Developer is recommended to provide a good support and information updates to all his client/consumer on the TOE especially on the security and critical updates related to the TOE security features and its supporting software running in the same environment as the TOE.

c) Developer is recommended to keep on updating the TOE user guide and relevant documentations based on latest information and features updates of the TOE. Thus, consumer/client is aware about the latest updates and information about the TOE.

d) Consumer/Client are advised to seek any help, assistance or guidance from developer of the TOE if in any cases of specific requirements shall be configured onto the TOE to meet certain policies, procedures and security enforcement within the consumer/client organization; thus, are recommended to seek details information directly from the developer. Therefore, there should not be any misconfiguration or malfunctions or insecure operations of the TOE that may affect consumer/client assets that is protected by the TOE.

e) It is recommended to run the TOE Mobile App on top of non-jailbroken iOS devices and non-rooted Android devices for better security and protections of malicious infections.

Annex A References

A.1 References

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

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

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

[4] MyCC Scheme Policy (MyCC_P1), v1c, CyberSecurity Malaysia, December 2015.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1b, December 2015.

[6] Security Target, Security Target for CENTAGATE, Version 3.0, 8 May 2017

[7] Evaluation Technical Report, E045 Evaluation Technical Report CENTAGATE, Version 3.0.10-build13, 15 May 2017

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

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

Acronym	Expanded Term
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 3: Glossary of Terms

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

Term	Definition and Source
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 ---