MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

C103 Certification Report

MyDigital ID version 1.1 (MyDigital ID Client v1.1 and MyDigital ID Server v1.1)

File name: ISCB-5-RPT-C103-CR-v1
Version: v1
Date of document: 19 November 2020
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

C103 Certification Report

MyDigital ID version 1.1 (MyDigital ID Client v1.1 and MyDigital ID Server v1.1)

19 November 2020
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:	C103 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C103-CR-v1
ISSUE:	v1
DATE:	19 November 2020
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 24 November 2020, 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	2 November 2020	All	Initial draft
d2	12 November 2020	Page 9-14	Edited on Section 2.1
v1	19 November 2020	Page 5	Edited on Figure 1 & Table 3

Executive Summary

The Target of Evaluation (TOE) is MyDigital ID v1.1 and consists of MyDigital ID Client v1.1 and MyDigital ID Server v1.1. The TOE is digital identity management and transaction signing platform. TOE provides convenient and secure method for third party mobile application to use the digital identity of mobile. The TOE implements the digital identity management and signing capability which is, reside as a mobile application that utilize the communication protocol and responsible for the message exchange between TOE client and TOE Server, via inter-app communication protocol on the mobile platform.

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 3 augmented with ALC_FLR.2 (EAL3+). 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.

The evaluation was performed by Securelytics SEF and the evaluation was completed on 30 October 2020.

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 MyDigital ID v1.1 (consists of MyDigital ID Server v1.1 and MyDigital ID Client v1.1) 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 TOE is MyDigital ID v1.1 which is consists of MyDigital ID Client v1.1 and MyDigital ID Server v1.1.

2 The TOE is a digital identity management and transaction signing platform.

3 The TOE provides convenient and secure method for third-party mobile applications to use the digital identity of mobile.

4 The TOE implements the digital identity management and signing capability which is, reside as a mobile application that utilize the communication protocol and responsible for the message exchange between TOE client and TOE server, via inter-app communication protocol on the mobile platform.

5 MyDigital ID Protocol defines the message exchange between the TOE client and TOE server via a third-party transaction server.

6 The protocol message consists of:

i) MyDigital ID Client

- Generate authorisation request as specified in the MyDigital ID protocol
- Verify the authorisation token issued by the MyDigital ID server as specified in the MyDigital ID protocol;
- Generate execution token (signed and encrypted), as specified in the MyDigital ID protocol

ii) MyDigital ID Server

- Interacting with the third-party transaction server via socket connection to communicate
- MyDigital ID protocol messages to the MyDigital ID client via third-party mobile application.
- Process the authorisation request generated by MyDigital ID client.
- Generate the authorisation token as specified in the MyDigital ID Protocol.
- Verify after decryption, the execution token generated by the MyDigital client
- Return transaction information to the third-party transaction server

7 The major security features of the TOE include:

a) Cryptographic Operation

b) Identification and Authentication

c) Data Protection

d) Communication

1.2 TOE Identification

8 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	C103
TOE Name	MyDigital ID
TOE Version	MyDigital ID v1.1 consist of MyDigital ID Server v1.1, and MyDigital ID Client v1.1
Security Target Title	MyDigital ID v1.1
Security Target Version	1.0
Security Target Date	30 September 2020
Assurance Level	EAL 3 augmented with ALC_FLR. 2 (EAL3+)
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
Sponsor	MIMOS Berhad Technology Park Malaysia 57000 Kuala Lumpur
Developer	MIMOS Berhad Technology Park Malaysia 57000 Kuala Lumpur

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

1.3 Security Policy

9 No organisational security policies have been defined regarding the use of the TOE.

1.4 TOE Architecture

10 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

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) Cryptographic Operation
The TOE provides elliptic curve (EC) key-pair generation, mutual client server authentication, digital signature generation and digital signature verification at both mobile application platforms and the digital identity Server.

b) Identification & Authentication
The third-party mobile application interconnected with the MyDigital ID client (TOE) is required to perform successful authentication before any information flow is permitted.

c) Data Protection
The TOE provides a secure storage capability for user digital certificates.

d) Communications
The TOE is able to protect the user data from disclosure and modification using a secure protocol that defines the message exchange between MyDigital ID client and MyDigital ID Server, via a third-party mobile application and third-party transaction server with additional security measures. Strong security characteristics with a stringent three-pass authentication mechanism for every transaction.

1.4.2 Physical Boundaries

12 The physical scope of the TOE includes:

i) MyDigital ID Client, and

ii) MyDigital ID Server

13 The TOE requires third-party mobile application (service application) and third-party transaction server (service provider) to operate as a complete IT solution for client organization as digital identity management platform (known as MyDigital ID Server).

14 The TOE is an authentication and transaction digital ID platform that enforces authentication, authorization, digital signing and the corresponding verification and validation processes through cryptography processes by offering mutual authentication, signature generation and correspondingly signature verification. The TOE offers signature generation, for the TOE client file and hash-data types.

15 The TOE allows the specified authentication process flows to be executed via supported mobile devices (for iOS and Android), on which the TOE client is installed.

16 The TOE client can be invoked from other mobile application (third-party service provider application) to consume the TOE security services, and furthermore leveraging its capability to provide a secure operational environment for private-key computations, inclusive of authentication and signature computation and protection of TOE Server and TOE client configuration.

17 Communication between TOE client and TOE server via MyDigital ID Communication Protocol through specific API proprietary requires by the TOE. This capability allows communication between both TOE components as well as involving communication internally between mobile applications (service provider mobile application and TOE client, as both resident on the mobile operating system) and internally at server side (between service provider transition server and TOE server).

18 Below are descriptions of the components stated in Figure 1:

Table 2: TOE Components based on Figure 1

Component	Description
MyDigital ID Client (TOE)	The TOE is the mobile application-server system as an authentication and transaction signing platform.
MyDigital ID Server (TOE)	The TOE Server implements the server side of MyDigital ID protocol and responsible for: i. Interacting with the third-party service provider via socket connection to communicate MyDigital ID protocol messages with the TOE application, as routed through the third-party service application and application-server connectivity;

	ii. Processing the authorisation request, in the form of the request token, generated by the TOE application; iii. Generating the authorisation token; iv. Processing the execution token generated by the TOE; and v. Return authentication information and status to the third-party service provider.
MyDigital ID Protocol	MyDigital ID Protocol defines the message exchange between the client and server via a third-party mobile application and third-party transaction server. It is based on three-pass authentication Mechanism MUT.CR as stated in N16813 ISO/IEC CD 9798-3.2019 with additional security measures, as stated in 11700-3.11 and 11700-6.7.
Third-party Mobile Application	Third-party Mobile Application is installed on the same mobile device and interacts with the TOE application to perform authentication and signing.
Third-party Transaction Server	Third-party server that communicates with the TOE server, for consumption of authentication and verification services.

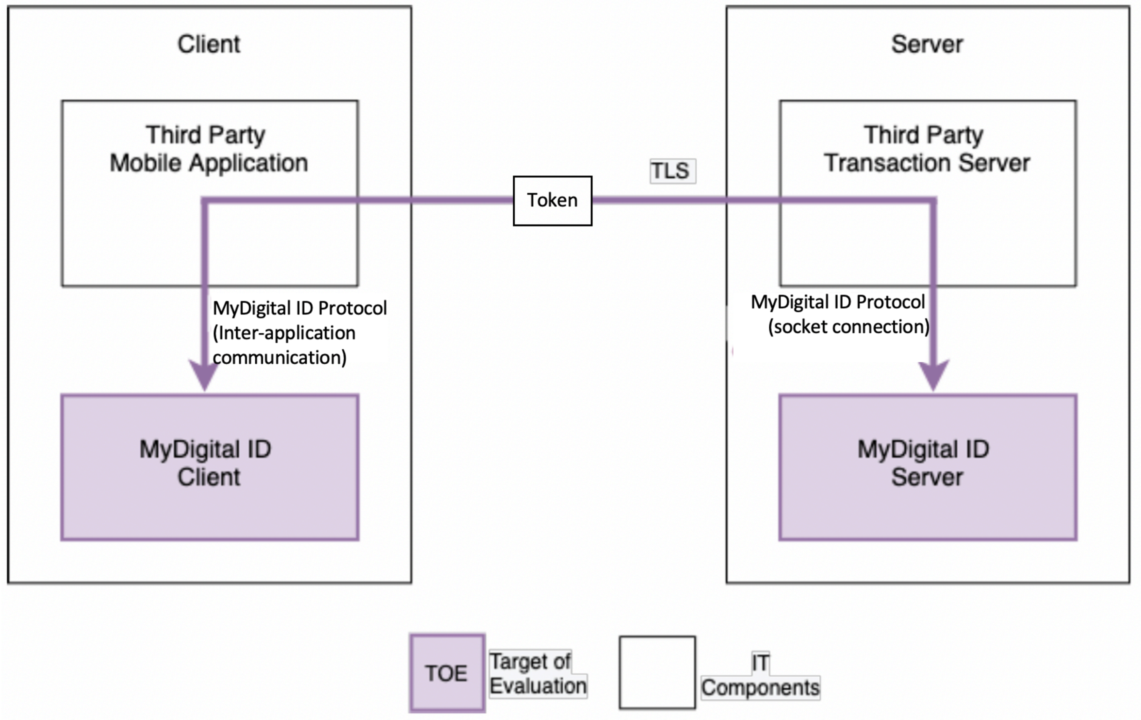
Client
Server
Third Party Mobile Application
Token
TLS
Third Party Transaction Server
MyDigital ID Protocol (Inter-application communication)
MyDigital ID Protocol (socket connection)
MyDigital ID Client
MyDigital ID Server
TOE
Target of Evaluation
IT Components

Figure 1: TOE physical boundary

1.5 Clarification of Scope

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

20 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]).

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

1.6 Assumptions

22 This section summarizes 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

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

a) A.ADMIN

The Service provider's administrator is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by MyDigital ID server documentation.

b) A.SERVER_OS

The operating systems supporting the TOE components protect against the unauthorised access, modification or deletion of the individual TOE components that they host.

c) A.UPDATE

The underlying platform on which the TOE operates will be regularly updated with the latest security patches and fixes to ensure data stored on the platform remains protected and secure.

d) A.NET_PORT

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

e) A.FIREWALL

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

f) A.MOBILE_OS

The TOE client user shall ensure not operating on jailbroken or rooted phone.

1.7 Evaluated Configuration

24 TOE operations are consist of two main parts:

a) Client, platform sitting on top of both iOS and Android operating system.

b) Server, reside in Server platform sitting on top on underlying operating system.

25 Even though the two main components reside in a separate platform, yet both of them are operates seamlessly to initiate secure communication and using proprietary communication protocol when TOE users requested to access the protected resources and the TOE itself.

26 Each of these main components is deployed in different platform in which consist of 2 sets of different hardware and software requirements. Thus, as for the TOE Server, which is the MyDigital ID Server is deployed in the Server environment either through server appliance mode or cloud-based system.

27 As for the TOE client, the TOE is the MyDigital ID Client are installed either on Android devices or iOS devices. This is depending on the devices recommended by the organization based on their security policies in the TOE deployment upon its secure operational environment.

1.8 Delivery Procedures

28 The evaluators examined the delivery procedure, in which provide guidance for the developer to initiate delivery process of the TOE and its components to the intended recipient(s). It is also provide direction on the methods used to deliver the TOE to consumers and users of the product.

29 The TOE shall be delivered by a trusted representative from Developer to End-User or intended recipient.

30 Before the TOE is delivered, all necessaries steps are performed by Developer representative, including:

- When the order is taken, Developer will send the release note to intended recipient (customer, end-user or etc.) by email for the release information (Product Name, Version and customer ID);
- Schedule is given out to intended recipient (customer, end-user or etc.) regarding the delivery of the TOE so that intended recipient can know when is the TOE is expected to be delivered by representative of Developer via email or phone call;
- A compresses and encrypted archive containing the TOE or packaged in form of physical smart card or relevant forms agreed by intended recipient customer, end-user or etc.) is produced by Developer and will be securely packaged in a box with seal; and
- The seal packaging securely will then be sent to the intended recipient (customer, end-user or etc.)
- For the mobile application on Android and iOS platform, it can be downloaded from Google Play Store and Apple App Store.

31 Upon received of the TOE in form of agreed by the recipient, the relevant parties required to sign and perform checking on the checklist provided by Developer. The form checklist shall be signed as acknowledgement of the received products as well as shall be returned back to Developer. Submission can be performed via email, postage and fax.

2 Evaluation

32 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 ISCB Scheme Requirement (MYCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

34 The evaluators checked that the TOE provided for evaluation is labelled with its reference.

35 The evaluators checked that the TOE references used are consistent.

36 The evaluators examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

37 The evaluators examined the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

38 The evaluators examined the CM access control measures described in the CM plan to determine that they are effective in preventing unauthorised access to the configuration items.

39 The evaluators checked that the CM documentation provided includes a CM plan.

40 The evaluators examined the CM plan to determine that it describes how the CM system is used for the development of the TOE.

41 The evaluators checked that the configuration items identified in the configuration list are being maintained by the CM system.

42 The evaluators checked the CM documentation to ascertain that it includes the CM system records identified by the CM plan.

43 The evaluators examined the evidence to determine that the CM system is being operated in accordance with the CM plan.

44 The evaluators checked that the configuration list includes the following set of items:

a) the TOE itself;

b) the parts that comprise the TOE;

c) the TOE implementation representation;

d) the evaluation evidence required by the SARs in the ST

45 The evaluators examines the configuration list to determine that it uniquely identifies each configuration items.

46 The evaluators checked that the configuration list indicates the developer of each TSF relevant configuration item.

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

48 The evaluators examined aspects of the delivery process to determine that the delivery procedures are used.

49 The evaluators examined the development security documentation to determine that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation.

50 The evaluators examined the development confidentiality and integrity policies in order to determine the sufficiency of the security measures employed.

51 The evaluators examined the development security documentation and associated evidence to determine that the security measures are being applied.

52 The evaluators examined the flaw remediation procedures documentation to determine that it describes the procedures used to track all reported security flaws in each release of the TOE.

53 The evaluators examined the flaw remediation procedures documentation to determine that the application of these procedures would produce a description of each security flaws in terms of its nature and effects.

54 The evaluators examined the flaw remediation procedures documentation to determine that the application of these procedures would identify the status of finding a correction to each security flaw.

55 The evaluators checked the flaw remediation procedures to determine that the application of these procedures would identify the corrective action for each security flaw.

56 The evaluators examined the flaw remediation procedures documentation to determine that it describes a means of providing the TOE users with the necessary information on each security flaw

57 The evaluators examined the flaw remediation procedures to determine that they describe procedures for the developer to accept reports of security flaws or request for correction to such flaws.

58 The evaluators examined the flaw remediation procedures to determine that the application of these procedures would help to ensure every reported flaw is corrected.

59 The evaluators examined the flaw remediation procedures to determine that the application of these procedures would help to ensure that the TOE users are issued remediation procedures for each security flaw.

60 The evaluators examined the flaw remediation procedures to determine that the application of these procedures would result in safeguards that the potential correction contains no adverse effects.

61 The evaluators examined the flaw remediation guidance to determine that the application of these procedures would result in means for the TOE user to provide reports of suspected security flaws or requests for correction to such flaws.

62 The evaluators examined the documented description of the life-cycle model used to determine that it covers the development and maintenance process.

63 The evaluators examined the life-cycle model to determine that use of the procedures, tools and techniques described by the life-cycle model will make the necessary positive contribution to the development and maintenance of the TOE.

2.1.2 Development

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

65 The evaluators examined the security architecture description to determine that it describes the security domains maintained by the TSF.

66 The evaluators examined the security architecture description to determine that the initialisation process preserves security.

67 The evaluators examined the security architecture description to determine that it contains information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities.

68 The evaluators examined the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

69 The evaluators examined the functional specification to determine that the TSF is fully represented.

70 The evaluators examined the functional specification to determine that it states the purpose of each TSFI.

71 The evaluators examined the functional specification to determine that the method of use for each TSFI is given.

72 The evaluators examined the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.

73 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.

74 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

75 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes error messages that may result from SFR-enforcing actions associated with each SFR-enforcing TSFI.

76 The evaluators examined the presentation of the TSFI to determine that it summarises the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

77 The evaluators checked that the tracing links the SFRs to the corresponding TSFIs.

78 The evaluators examined the functional specification to determine that it is a complete instantiation of the SFRs.

79 The evaluators examined the functional specification to determine that it is an accurate instantiation of the SFRs.

80 The evaluators examined the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.

81 The evaluators examined the TOE design to determine that all subsystems of the TSF are identified.

82 The evaluators examined the TOE design to determine that each SFR-non-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-non-interfering.

83 The evaluators examined the TOE design to determine that it provides a complete, accurate and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

84 The evaluators examined the TOE design to determine that it provides a complete and accurate high-level description of the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems.

85 The evaluators examined the TOE design to determine that it provides a complete and accurate high-level description of the behaviour of the SFR-supporting subsystems.

86 The evaluators examined the TOE design to determine that interactions between the subsystems of the TSF are described.

87 The evaluators examined the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

88 The evaluators examined the TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered by the TOE design.

89 The evaluators examined the TOE design to determine that it is an accurate instantiation of all security functional requirements.

2.1.3 Guidance Documents

90 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

91 The evaluators examined the operational user guidance to determine that it describes, for each user role, the secure use of the available interfaces provided by the TOE.

92 The evaluators examined the operational user guidance to determine that it describes, for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

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

94 The evaluators examined the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

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

96 The evaluators the operational user guidance to determine that it is clear and reasonable.

97 The evaluators examined the provided acceptance procedures to determine that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

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

99 The evaluators performed all user procedures necessary to prepare the TOE to determine that the TOE and its operational environment can be prepared securely using only the supplied preparative procedures.

2.1.4 IT Product Testing

100 Testing at EAL 3+ consists of assessing developer tests, sufficiency test and conducting penetration tests. The TOE testing was conducted by evaluators from Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

a) 2.1.4.1 Assessment of Developer Tests

101 The evaluators verified that the developer has met their testing responsibilities by repeating the 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.

b) 2.1.4.2 Independent Test

102 At EAL 3+, independent test demonstrates the correspondence between the security functional requirements (SFRs) defined in Security Target, and the test cases that test the functions and behaviour of the TOE that meets those requirements. The evaluators have decided to perform testing based on the TOE Security Functions.

103 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 developed and performed by the evaluators to verify the functionality as follows:

Table 3: Functional Test

Test ID	Description	SFRs	Results
F001 – Identification and Authentication, Cryptographic Operation & Data TSFI: 3rd Party Service Application 3rd Party Service Provider Cryptographic Server Engine	1. To test that each MyDigital ID client and MyDigital ID Server are successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user 2. To test that the TOE generates the below cryptographic keys in accordance with a specified cryptographic key generation algorithm: AES 256 bit, ECDSA 256 bit, ECDH 256 bit 3. To test that the TOE performs digital signature creation and verification in accordance with a specified cryptographic algorithm: • ECDSA with SHA-2, • AES with cryptographic key sizes:	FIA_UAU.2 FIA_UID.2 FCS_COP.1 FCS_CKM.4 FCS_CKM.1	Pass

	- ECDSA using secp256r1 curve of 256 bits over Fp and SHA-2 256 bits, - AES 256 bit 4. To test that the TOE destroys cryptographic keys in accordance with a specified cryptographic key		
F002- Cryptographic Operation & Data Protection TSFI: Cryptographic Server Engine	1. To test that the TOE distributes cryptographic keys in accordance with a specified cryptographic key distribution method · X.509 public key certificate in PKCS #7 format, · PKCS #10 certificate request	FCS_CKM.2 FDP_DAU.1 FCS_COP.1 FCO_NRO.1.1	Pass
F003 – Cryptographic Operation TSFI: Cryptographic Server Engine	1. To test that the TOE provides a capability to generate evidence that can be used as a guarantee of the validity of document signed 2. To test that the TOE provides the signatory with the ability to verify evidence of the validity of the indicated information 3. To test that the TOE able to generate evidence of origin for transmitted (certificates) at the request of the recipient 4. To test that the TOE be able to relate the client ID, public key, signature algorithms of the originator of the information and the certificate serial ID, sequence identifier, identifier ID, public key, signature algorithm of the information to which the evidence applies.	FCS_CKM.2 FDP_DAU.1 FCS_COP.1 FCO_NRO.1.1	Pass
F004 – Secure Communication	1. To test that the TOE provides a communication path between itself and remote IT Systems that is logically distinct	FTP_TRP.1.1	Pass

TSFI: TLS_API	from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure		

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

c) 2.1.4.3 Vulnerability Analysis

105 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.

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

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

b) Specialist technical expertise required (specialist expertise);

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

d) Window of opportunity; and

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

d) 2.1.4.4 Vulnerability testing

107 The penetration tests focused on:

i) Tamper the file & message during digital signing

ii) Unauthorized mobile application

iii) PIN Lockout

iv) Information Leakage – Log Analysis (Server)

v) Information Leakage – Folder

vi) Information Leakage – Log Analysis (Mobile)

vii) Improper error message handling

viii) Information leakage during transmission

ix) Information leakage in the shared storage

x) Server Misconfiguration – File Upload

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

e) 2.1.4.5 Testing Results

109 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 tests conducted were PASSED as expected.

3 Result of the Evaluation

110 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 MyDigital ID version 1.1 (MyDigital ID Client v1.1 and MyDigital ID Server v1.1) which is performed by Securelytics SEF.

111 Securelytics SEF found that MyDigital ID version 1.1 (MyDigital ID Client v1.1 and MyDigital ID Server v1.1) upholds the claims made in the Security Target (Ref [6]) and supporting documentations and has met the requirements of the Common Criteria (CC) assurance Level 3 Augmented with ALC_FLR.2 (EAL3+ ALC_FLR.2).

112 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

113 EAL 3+ 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 behaviour.

114 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 an attacker possessing Enhanced-Basic attack potential.

115 EAL 3+ ALC_FLR.2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

116 It is strongly recommended that:

- 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.
- 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.
- 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

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, Dec 2019.

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

[6] MyDigital ID v1.1 Security Target, Version 1.0, 30 September 2020.

[7] Evaluation Technical Report MyDigital ID, Version 1.0, 30 October 2020.

A.2 Terminology

A.2.1 Acronyms

Table 4: 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
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 5: 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.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.

Term	Definition and Source
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 ---