MINISTRY OF DIGITAL

C136 Certification Report

HumanCard Ver. 3.1

File name: ISCB-5-RPT-C136-CR-v1
Version: v1
Date of document: 29 July 2025
Document classification : PUBLIC

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

CyberSecurity Malaysia
200601006881 (726630-U)
www.cybersecurity.my

Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
T +603 8800 7999 F +603 8008 7000 H 1 300 88 2999

C136 Certification Report

HumanCard Ver. 3.1

29 July 2025

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:	C136 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C136-CR-v1
ISSUE:	v1
DATE:	29 July 2025
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. 200601006881 (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 set of 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.

The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) https://iscb.cybersecurity.my/index.php/certification/product-certification/mycc/ and the Common Criteria Recognition Arrangement at http://www.commoncriteriaportal.org

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	04 July 2025	All	Initial draft
v1	29 July 2025	All	Final Version

Table of Contents

Index of Tables

Index of Figures

Executive Summary

The project is C136 HumanCard Ver. 3.1, referred to as the Target of Evaluation (TOE) which developed by HumanCard Technology Sdn Bhd. The TOE is a modernized business card with digitalisation capabilities that equipped with contactless smart card technology, which is NFC that allows the custodian of the card to shared information of their credentials through NFC contactless reading via mobile phone(s) with NFC reader feature.

With the modernised digital business card approached, the needs of having paper based business card and creating unnecessary waste upon losing the business card, custodian of HumanCard as the digital business card able to share their information and credentials such as phone number, address, links to social media, videos of advertisement related to their company etc. that can be reachable through online browser upon scanning the card via NFC reader on their mobile phone. All information and credentials can be presented in the format of images, videos etc. through the profile of the custodian projected on the Web App hosted by HumanCard.co.

The TOE provides security functions such as Identification and Authentication, Security Management, Secure Access and NFC Data Tampering Protection.

The scope of the evaluation is defined by the Security Target ([6]) which identifies 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 1 (EAL1). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was conducted by CyberSecurity Malaysia MySEF (CSM MySEF) and was completed with the submission of the Final Evaluation Technical Report (ETR) on 30 June 2025.

This certification report is associated with the product evaluation certificate issued on 7 Aug 2025 and the Security Target (Ref [6]). The certification will expire five (5) years from the date of certificate issuance.

It is the responsibility of the user to ensure that HumanCard Ver. 3.1 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.

1 Target of Evaluation

1.1 TOE Description

1 The HumanCard is a modernised smart card with embedded NFC chip that allows TOE User to scan the card via mobile phone through NFC reader or scanning the surface of the card that printed with unique QR code, in which both interfaces linked to the personalised Web App containing information and credentials of the TOE User as the card custodian.

2 The Web App of the TOE is hosted by TOE Developer that allow TOE User to login into their dedicated account to personalise their content, information and credentials that will be viewed by the anyone that scan the card presented by the TOE User to anyone or via scanning the QR code. Whilst, as for the TOE management and TOE operations are accessible by the TOE Developer.

3 The TOE are consist of two parts:

i. TOE Web App.

ii. TOE NFC Card.

The address of the TOE Web App can be accessible via URL: https://humancard.me

4 Note that, the link https://humancard.co/ is a commercial website of HumanCard, not the TOE Web App.

5 For TOE NFC Card, the embedded link in the TOE NFC Card are in the scope of evaluation. The embedded link is a unique link created by the TOE Web App for the TOE User that be scan by intended recipient of the card using NFC reader (such as, smartphone with NFC reader) or QR Code scanner to view the TOE User personalised Web App that shown all the details related to TOE User content, credentials, links etc. shared information allowed by the TOE User.

6 The excluded scope of evaluation are being stated below.

i. QR Code generated by the TOE Web App.

ii. Cloud platform hosting the TOE Web App.

iii. NFC hardware chip, NFC antenna and its hardware including the physical card material.

iv. Mobile phone and its NFC reader.

Note that, the TOE Developer role in this document is defined the product developer and not related to TOE User Admin or TOE User. And does not part of the scope of TOE.

1.2 TOE Identification

7 The details of the TOE are identified in table below.

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C136
TOE Name	HumanCard
TOE Version	Ver. 3.1
Security Target Title	HumanCard Ver. 3.1 Security Target
Security Target Version	v1.3
Security Target Date	26 May 2025
Assurance Level	Evaluation Assurance Level 1
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 1
Sponsor	HumanCard Technology Sdn Bhd 14 Jalan TPK 1/6, Taman Perindustrian Kinrara, 47100 Puchong, Selangor.
Developer	HumanCard Technology Sdn Bhd 14 Jalan TPK 1/6, Taman Perindustrian Kinrara, 47100 Puchong, Selangor.
Evaluation Facility	CyberSecurity Malaysia MySEF Level 7, Tower 1, Menara Cyber Axis, Jalan Impact,

	63000 Cyberjaya, Selangor Darul Ehsan, MALAYSIA

Table 1: TOE Identification

1.3 Security Policy

8 No Organisational Security Policy (OSP) declared for the TOE.

1.4 TOE Architecture

9 The TOE consist of logical and physical boundaries which are described in Section 1.5 of the Security Target ([6]).

1.4.1 Logical Boundaries

10 The logical boundary of the TOE is summarized below:

- **Identification and authentication**
  TOE has the capabilities to enforces all TOE User to key in their registered credentials consist of username (email address) and password in allowing them to access the TOE Web App. Upon successfully identification and authentication of TOE User, all of them shall be able to access their individual web app page for them to create, modify and delete any information, credentials and data which that can be view by anyone that has access to the unique link embedded in the NFC chip and QR code.
  The same method of login is applicable to TOE User Admin to access the TOE Web App that have additional menu and access related to the admin privilege.

- **Security management**

  The TOE has the management functions that operates the TOE overall operation including managing all TOE user accounts consist of TOE User Admin and the TOE User, managing unique link to the TOE User profile, and assignment of TOE NFC Card to the TOE User profile. Also, the TOE User Admin ensure all TOE User able to have access to their account as well as anyone that have access to link via TOE NFC Card or QR code are able to view the link upon scanning.

For TOE User, as the custodian of the TOE NFC Card, only can access their profile in the TOE Web App with authorisation of updating their own data, contents, information and credentials.

- **Secure Access**

  TOE enforce secure access via HTTPS enable provided by the AWS securityprotection mechanism in ensuring all data transmitted between TOE Web App and any internet browser(s) within the mobile phone or any platform are securely protected.

  The access to the TOE Web App and the TOE Web App User Profile uniquely personalised for the TOE User, which are both protected by the HTTPS, whilst also protected from possible unvalidated changes made on the TOE (possible changes made without confirmation by TOE User or TOE User Admin).

  In addition, action taken by TOE User Admin and TOE User via selecting logout function will automatically terminate the session and any unsaved action will not be enforced on the TOE.

- **NFC Data Tampering Protection**

  Each TOE NFC Card has been personalised by TOE Developer based the request made by TOE User Admin. In each personalised TOE NFC Card embedded a unique link securely protected with permanent read-only access without enabling the write access. This mechanism is to protect the data embedded inside the NFC chip from being overwritten and any forms of data manipulation on the linked personalised on the NFC chip. Note that, the TOE NFC Card that has been personalised for the TOE User can’t be repersonalised as the overwrite mode for the NFC chip has been locked.

1.4.2 Physical Boundaries

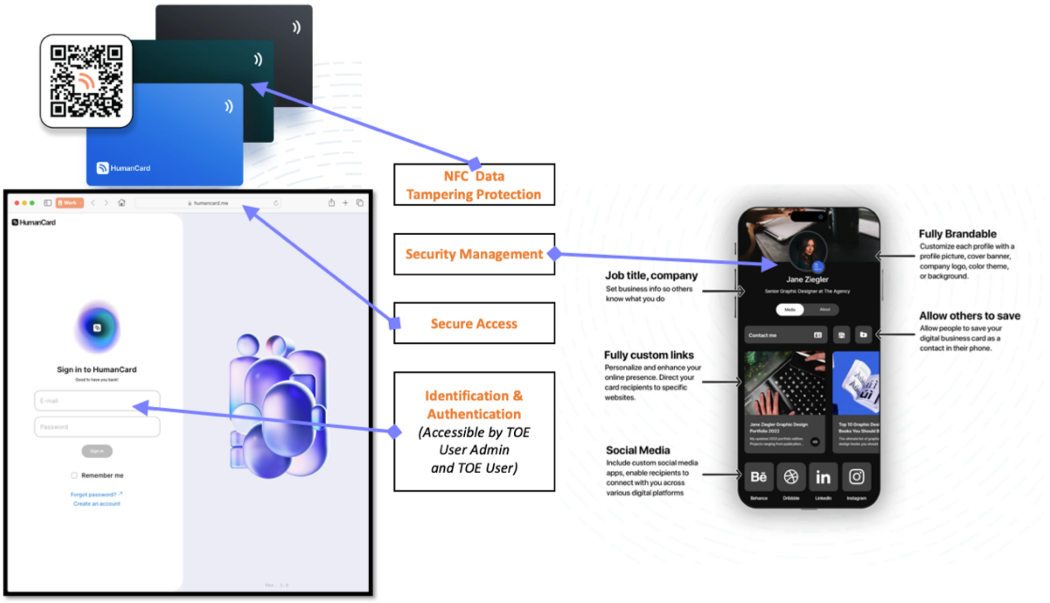
HumanCard
NFC Data Tampering Protection
Security Management
Secure Access
Identification & Authentication (Accessible by TOE User Admin and TOE User)
Sign in to HumanCard
E-mail
Password
Sign in
Remember me
Forgot password?
Create an account
Job title, company
Set business info so others know what you do
Fully custom links
Personalize and enhance your online presence. Direct your card recipients to specific websites.
Social Media
Include custom social media apps, enable recipients to connect with you across various digital platforms
Jane Ziegler
Senior Graphic Designer at The Agency
Media
About
Contact me
Behance
Dribbble
LinkedIn
Instagram
Fully Brandable
Customize each profile with a profile picture, cover banner, company logo, color theme, or background.
Allow others to save
Allow people to save your digital business card as a contact in their phone.

Figure 1: Actual Image of the TOE and Evaluation Scope

11 Above in the Figure 1 has highlighted in ORANGE FONT is the scope of the TOE.

12 The TOE consist of two (2) parts, which are the TOE Web App that operates under the purview of TOE Developer through the authorised TOE configuration and the TOE operations managed by the TOE Developer via the TOE Web App hosted by the TOE Developer. In which, the TOE Web App is hosting all the contents, credentials and information about the TOE User, as custodian of the TOE NFC Card holds by the TOE User as their modernised digital business card.

13 The TOE Web App operates via hosted server located in the AWS public cloud by the TOE Developer. In terms of managing the TOE, the TOE Developer will be the main representative of the TOE Developer to operate the TOE from the management and operations perspectives of the TOE Configuration within the TOE operations.

14 The TOE User admin is a representative of an authorised administrator appointed by the organization. The creation of TOE User Admin account is performed via self-registration in the TOE Web App. Once the account has been created, the TOE Developer will upgrade the account privilege as TOE User Admin account.

15 The TOE User Admin are allowed to manage all the TOE User accounts registered in the TOE Web App based on the subscription by the organisation. The subscription of

the TOE are based on the TOE NFC Card quantity. The TOE User Admin shall activate and assign the TOE NFC Card to the TOE User.

16 As for the TOE User, the TOE User Admin shall invite the TOE User as members of the organisation by adding their email in the organisation group list. The invitation process also can be perform by importing list of emails from a .CSV format file. The TOE will send an invitation email with login details to the new user.

17 The TOE Web App is by the TOE User accessible from the perspectives of managing their profile created based on the account that contain their own information, content and credentials as registered TOE User of the TOE Web App.

18 As for the TOE NFC Card, consist of physical NFC card that printed with basic information about the TOE User on top of the card inclusive of the QR code (upon request by TOE User) and TOE embedded inside the NFC chip that contained unique link that shall be triggered upon reading/scanning of NFC reader via mobile phone. The link that personalised on the NFC chip are protected and can't be overwritten. The TOE NFC Card that has been personalised by TOE Developer and delivered to the TOE User is unable to be re-personalised as the overwrite mode for the NFC Chip has been permanently locked. Note that, the scope of evaluation covers only the data (which is the unique linked) stored/embedded inside the NFC chip protected by the read and write protocol communication of NFC based on ISO/IEC standards related to contactless smart card.

19 The operation of the TOE of both parts triggered when any person scan/read the NFC chip embedded on the TOE NFC Card using mobile phone NFC reader or scanning the QR code scanner app using any form of QR code scanner or mobile phone camera, whilst disclose the URL links to the TOE User personalised Web App that shown all the details related to TOE User content, credentials, links etc. shared information allowed by the TOE User.

20 Furthermore, TOE User able to customise and update their details, contents and credentials of their profile by login to the TOE Web App (https://humancard.me) using their registered username (email address) and password. The TOE Web App are deployed on the AWS cloud environment protected by AWS security protections with enable HTTPS.

1.5 Clarification of Scope

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

22 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]).

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

1.6 Assumptions

24 This section is not applicable for EAL1.

1.7 Evaluated Configuration

25 This section describes the evaluated configurations of the TOE that are included within the scope of the evaluation.

26 The TOE is configured according to the Preparative Guidance documents.

27 The TOE consists of two (2) parts, which are the TOE Web App that can be accessed via URL: https://humancard.me and TOE NFC Card.

28 TOE NFC Card, the embedded link in the TOE NFC Card are in the scope of evaluation. The embedded link is a unique link created by the TOE Web App for the TOE User that be scan by intended recipient of the card using NFC reader (such as, smartphone with NFC reader) or QR Code scanner to view the TOE User personalised Web App that shown all the details related to TOE User content, credentials, links etc. shared information allowed by the TOE User.

29 The The minimum requirements for Mobile Phone and Desktops are as following:

i. Mobile Phone Type: Equipped with NFC reader, QR code scanner and internet browser accessible with internet.

ii. Desktop with internet browser: Installed with Internet browser that have intenet access that able to browse the Web App URL (https://humancard.me)

30 For evaluation purposes, the testing conducted using an environment configured according to the baseline defined in the Guidance documents. The detailed configuration used during the testing are as following:

a) Mobile Phone

<u>Pixel 6 Pro</u>

i. Memory: 128GB

ii. NFC enabled: Yes

iii. Android Version: 12

POCO X4 Pro 5G

i. Memory: 256GB

ii. NFC enabled: Yes

iii. Android Version: 12

b) Desktop

Dell Precision 5820 Tower

i. Operating System: Windows

ii. RAM: 32GB

iii. Browser: Chrome

31 The TOE NFC card is delivered to TOE user via package courier.

1.8 Delivery Procedures

32 This section in not applicable for EAL1.

2 Evaluation

33 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 1. 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

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

2.1.1 Life-cycle support

35 The evaluator found that the TOE provided for evaluation is labelled with its reference.

36 The evaluator checked that the TOE references use are consistent.

37 The evaluator examined the configuration list to determine that it uniquely identifies each configuration item.

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

2.1.2 Development

39 The evaluator examined the functional specification, which describes the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

40 The evaluator examined the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

41 The evaluator verified that the SFRs are traced to the TSFIs in the functional specification.

42 The evaluator determined that the functional specification is accurate and complete instantiation of the SFRs.

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

2.1.3 Guidance documents

44 The evaluator 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.

45 The evaluator examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

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

47 The documents for TOE users to refer as guidance are as per listed:

i. HumanCard Ver. 3.1 Teams User Guide v1.4

ii. HumanCard Ver. 3.1 User Guide v1.4

2.1.4 IT Product Testing

48 Testing at EAL 1 consists of performing independent functional test and conducting penetration tests. The TOE testing was conducted by CyberSecurity Malaysia MySEF. The detailed testing activities including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report (TPR).

2.1.4.1 Independent Functional Testing

49 At EAL 1, provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

50 All an evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.

NO.	TEST TITLE	DESCRIPTION	SECURITY FUNCTION REQUIREMENT	TSFI
TEST GROUP A: Identification and Authentication				
1.	A1. Create Account (TOE User Admin)	To test whether the TOE User Admin can create account via self-registration in the TOE.	FIA_ATD.1 FMT_SMR.1	Internal TSFI 1
2.	A2. First time login (TOE User)	To test whether the TOE User can login for the first time after invited by the organization through email.	FIA_UID.2 FIA_UAU.2 FMT_SMR.1	Internal TSFI 1
3.	A3. Login using correct credential	To test whether user can login to the TOE using the correct username and password.		
4.	A4. Login using incorrect credential	To test whether user can login to the TOE using the incorrect username and/or incorrect password.		
TEST GROUP B: Security Management				
5.	B1. Create User Account (TOE User Admin)	To test whether TOE User Admin can manage TOE User Account (create, modify and delete)	FMT_SMF.1 FMT_SMR.1 FMT_MTD.1 FIA_ATD.1	Internal TSFI 1 Internal TSFI 2
6.	B2. Manage Unique Link (TOE User Admin)	To test whether TOE User Admin can manage unique link to the TOE User profile (create and delete)	FMT_SMF.1	Internal TSFI 1 Internal TSFI 2
7.	B3. Assign TOE NFC Card (TOE User Admin)	To test whether the TOE User Admin can assign the TOE NFC card to the TOE User (create)	FMT_SMF.1 FIA_ATD.1	Internal TSFI 2 Internal TSFI 3 External TSFI

NO.	TEST TITLE	DESCRIPTION	SECURITY FUNCTION REQUIREMENT	TSFI
8.	B4. Unassign TOE NFC Card (TOE User Admin)	To test whether the TOE User Admin can manage the TOE NFC card to the TOE User (delete)		Internal TSFI 1 Internal TSFI 2
9.	B5. Modify User Profile (TOE User)	To test whether TOE User can modify and update their profile.	FMT_MTD.1	Internal TSFI 1 Internal TSFI 2
10.	B6. Add User Profile (TOE User)	To test whether TOE User can add new profile		
11.	B7. Delete User Profile (TOE User)	To test whether TOE User can delete and clear their own profile.		
TEST GROUP C: Secure Access				
12.	C1. Trusted channel (HTTPS)	To test whether the TOE communication initiated via the trusted channel (HTTPS)	FTP_ITC.1 FTA_TSE.1	External TSFI 2
13.	C2. User terminate session	To test whether the TOE allow user-initiated termination of the user's own interactive session.	FTA_SSL.4	External TSFI 2
TEST GROUP D: Data Tamper Protection				
14.	D1. Overwrite data in NFC Card	To test whether the TOE NFC card cannot be overwritten. (FRU_FLT.1)	FPT_FLS.1 FRU_FLT.1	External TSFI 1

Table 2: Independent Functional Test

51 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.

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

2.1.4.2 Vulnerability Analysis

53 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.

54 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

2.1.4.3 Vulnerability testing

55 The penetration tests focused on:

a) Authentication Bypass

b) Sensitive Data Exposure in HTTPS Transmission

c) Broken Access Control

d) Network Sniffing

e) Insecure Session Termination

f) Overwrite data in NFC Card

g) Cross Site Scripting (XSS)

56 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]).

2.1.4.4 Testing Results

57 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 Results of the Evaluation

58 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 HumanCard Ver. 3.1 which is performed by CyberSecurity Malaysia MySEF.

59 CyberSecurity Malaysia MySEF found that HumanCard Ver. 3.1 upholds the claims made in the Security Target (Ref **Error! Reference source not found.**) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 1.

60 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

61 EAL 1 provides a basic level of assurance by a limited security target and analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

62 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

63 EAL 1 also provides assurance through unique identification of the TOE and the relevant evaluation documents.

64 This EAL provides a meaningful increase in assurance over unevaluated IT.

3.2 Recommendation

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

a) Opinions and interpretations expressed herein are outside the scope of certifcation.

b) It is recommended that the developer continue updating the TOE User Guide and relevant documentation to reflect any new or updated TOE features.

Annex A

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), v2, April 2025.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v4, April 2025.

[6] HumanCard Ver. 3.1 Security Target, v1.3, 26 May 2025.

[7] CyberSecurity Malaysia MySEF E053 Evaluation Technical Report HumanCard Ver. 3.1, v1, 30 June 2025.

A.2 Glossary

A.2.1 Abbreviations

Table 3: List of Abbreviations

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

Acronym	Expanded Term
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 Terminology

Table 4: Terminology

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 ---