HumanCard Ver. 3.1 Security Target

Common Criteria: EAL1

Document Version : 1.3

Document Date : 26 May 2025

Document management

Document identification

Document title	HumanCard Ver. 3.1 Security Target
Document version	1.3
Document date	26 May 2025
Author	Securelytics.my
Release Authority	HumanCard

Document history

Version	Date	Description
0.1	5 JAN 24	Initial draft.
0.2	16 JAN 24	Updated based on comments by SEF on initial review.
0.3	21 FEB 24	Updated based on comments by SEF on EOR.
0.4	8 APR 24	Updated based on comments by SEF on EOR.
0.5	19 APRIL 24	Updated based on comments by SEF on EOR.
0.6	24 MAY 24	Updated based on comments by SEF on EOR.
0.7	18 JULY 24	Updated based on comments by SEF and CB on EOR.
0.8	26 AUG 24	Updated based on comments by SEF on EOR.
0.9	4 NOV 24	Updated based on comments by SEF on EOR.

Version	Date	Description
0.10	5 NOV 24	Updated based on comments by SEF on EOR.
1.0	5 NOV 24	Final Released.
1.1	19 FEB 25	Final Released. Updated TOE.
1.2	22 APR 25	Updated TOE.
1.3	26 MAY 25	Minor Changes. Final Released.

Table of Contents

1 SECURITY TARGET INTRODUCTION

1.1 ST Reference

Doc Title	HumanCard Ver. 3.1 Security Target
Doc Version	1.3
Doc Date	26 May 2025

1.2 TOE Reference

TOE Title	HumanCard
TOE Version	Ver. 3.1

1.3 Defined terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term	Description
Authentication data	It is information used to verify the claimed identity of a user.
ACL	Access control lists
NFC	Near Field Communication
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
Unauthorised user	An unauthorised user is an individual that does not have authorisation to use the functionality of the TOE.
TOE Developer	TOE Developer is known as the product developer for the TOE. This role known as the developer of the TOE and manage the operations of the TOE. This role is outside the scope of TOE evaluation and certification.

Term	Description
TOE User Admin	TOE User Admin as representative of the TOE User and representative of authorised administrator of client/customer/subscriber of the TOE that able to manage all the TOE User.
TOE User	TOE User that has a registered account in the TOE and being managed by the TOE User Admin.
User data	Data created by and for the TOE User, which may or does not affect the operation of the TSF.

1.4 TOE Overview

1.4.1 TOE Usage and major security functions

HumanCard as the Target of Evaluation (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.

Alternatively, HumanCard also has the similar features of the common paper based business card that allow to engrave all the basic information of the card custodian on the surface of the card. Including QR code that can be scannable and shareable with any person in contact with the card. This is an alternative method of sharing information with others did not have NFC reader on their phone. By scanning the QR code, the link embedded in the QR will trigger the mobile phone browser to open the Web App hosted by HumanCard.co related to the custodian of the card.

The following table highlights the range of security functions implemented by the TOE.

Table 1: TOE Security Functions

Security Function	Description
Identification and Authentication	The TOE has the capability to enforce access control based on identification and authentication through the usage of username (email address) and password on the Web App for TOE User and TOE User Admin to access their personalisation page of their information and credentials.
Security Management	The TOE has the capabilities to manage all the details, information, credentials related to the TOE User Admin, within the TOE configuration and the TOE operations managed via the TOE Web App hosted by the TOE Developer. The TOE are being managed by the TOE Developer via TOE Web App. The TOE Web App is accessible by TOE User Admin to manage their organisation TOE User by assigning TOE User to a profile with unique link in the TOE Web App.

Security Function	Description
	The TOE also provide access to TOE User to manage their profile that contain credentials such as phone number, address, links to social media, videos of advertisement related to their company etc. in the Web App upon successful login to the Web App.
Secure Access	The TOE has the capabilities to enforce secure access to the TOE Web App hosted by the TOE Developer by enabling HTTPS that protect the data transmitted between TOE User internet browser(s) with the TOE Web App containing the TOE User information and credentials. In addition, the logged on session of TOE User and TOE User Admin shall be terminated upon selecting logout function.
NFC Data Tampering Protection	The TOE has the capability to prevent basic tampering on data embedded in the NFC chip by preventing the attempt to overwrite the existing data with manipulate data with the intention of manipulating it with malicious intent.

1.4.2 TOE Type

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.

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.

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

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

Note that, 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.

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.

1.4.3 Non-TOE Supporting Hardware, Software and/or Firmware.

The following are the list of supporting hardware, software and/or firmware required by the TOE to operate, in which are not part of TOE scope of evaluation.

Table 2: Minimum System Requirements for TOE

Minimum System Requirements	
TOE NFC Card	
NFC Chip	Any type of NFC chip that are compliance to the requirements of communication protocol defined by the following ISO/IEC standards: i. ISO/IEC 18092 / ECMA-340—Near Field Communication Interface and Protocol-1 (NFCIP-1)[63] ii. ISO/IEC 21481 / ECMA-352—Near Field Communication Interface and Protocol-2 (NFCIP-2); and iii. Support the protocol communication of ISO/IEC 14443:2016 Part 1 – Part 4.
Card Material	Card in the form of contactless smart card that are using a range of plastic materials such as PVC, PET, PETG, PC and ABS, or non-magnetic metal that safe to use by human.
Web Server Hosting – Cloud Platform	

Minimum System Requirements	
Cloud Platform	AWS
Server Operating System	Windows Based or Linux Based Operating System (OS) based on the EC2 instances made available in the virtual machine library of AWS. Note that, the selection of OS is based on the secure implementation and security updates enable and supported by AWS.
Server CPU	Min. of 8 vCPU for the virtual machine (auto-scaling).
Server RAM	Min. of 16GiB for RAM for the virtual machine (auto-scaling).
Server Hard Disk	Min. of 500G vHDD for the virtual machine (auto-scaling).
Server Internet Access	Enabled and protected by WAF AWS.
Mobile Phone	
Mobile Phone Type	Equipped with NFC reader, QR code scanner and internet browser accessible with Internet.
Desktop	
Desktop with Internet Browser	Installed with Internet Browser that have Internet access that able to browse the Web App URL: https://humancard.me

1.5 TOE Description

1.5.1 Physical scope of the TOE

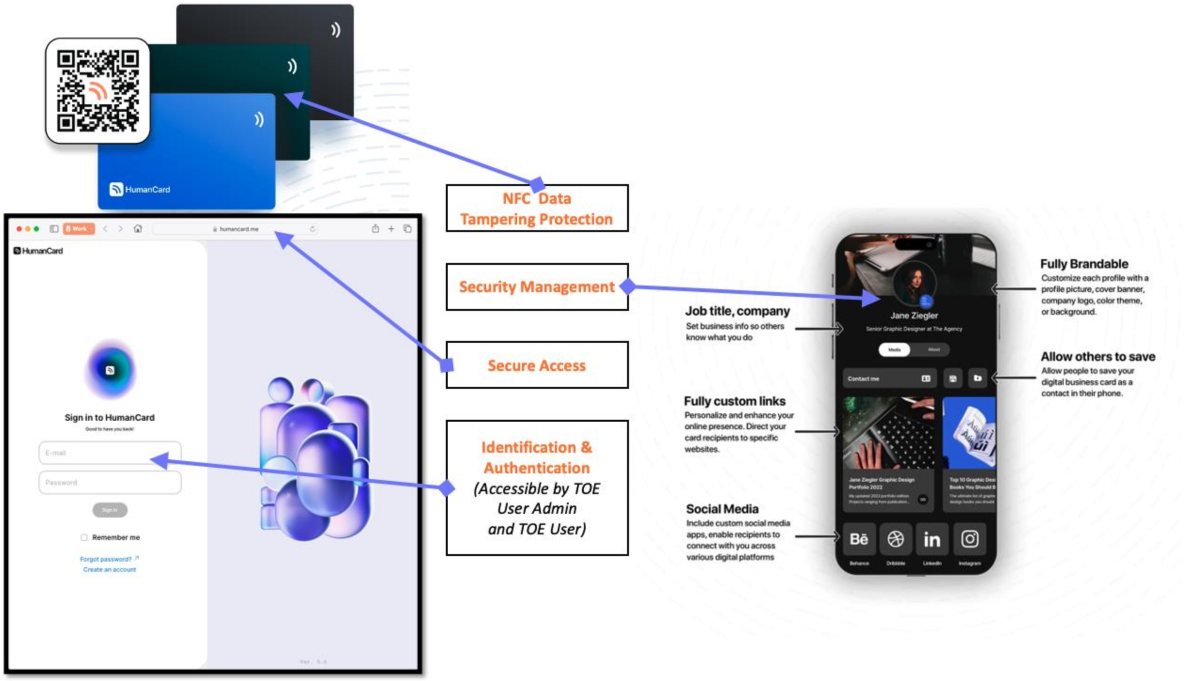
HumanCard
NFC Data Tampering Protection
Security Management
Secure Access
Identification & Authentication (Accessible by TOE User Admin and TOE User)
Sign in to HumanCard
E-mail
Password
Sign in
Remember me
Forgot password?
Create an account
Jane Ziegler
Senior Graphic Designer at The Agency
Contact me
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
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.
Behance
Dribbble
LinkedIn
Instagram

Figure 1 – Actual Image of the TOE and Evaluation Scope

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

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.

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.

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.

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.

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.

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.

Note that, all access to the TOE Web App are using the method of secure communication using HTTPS are enable for TOE Web App and also during accessing the TOE User profile page upon reading the NFC Card or QR Code scanning.

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 as stated in Section 1.4.3.

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.

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.

Each user profile are associated with 1 TOE NFC Card. Each TOE NFC Card is consider as 1 HumanCard NFC Card.

In addition, the procured TOE NFC Card will be delivered to TOE User using package courier. The card can be use directly without configuration before use. The delivery of the TOE NFC Card are being performed by TOE Developer.

The TOE Web App is hosted and managed by the TOE Developer, in which is support team of the TOE Developer in ensuring the TOE Web App is always accessible, configured securely and all contents, data, credentials etc. are well protected under the security protection of AWS via HTTPS protocol secure communications.

The TOE can operates within the computing environment that based on the minimum requirements of the TOE defined in section 1.4.3.

Aside of the guidance documentation, TOE can be provision from TOE Developer through a request via email, in which the TOE will be delivered to the TOE User based on the TOE delivery procedure.

Note that, all the components stated in section 1.4.2 (excluded in TOE scope of evaluation) and section 1.4.3 in this document shall be treated as not part of the TOE scope.

1.5.2 Logical scope of the TOE

The following is the list of TOE logical scope that defined in this document, covers by the Security Functional Requirements (SFRs).

A. **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.

B. **Security Management.** 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.

C. **Secure Access.** TOE enforce secure access via HTTPS enable provided by the AWS security protection 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.

D. **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 re-personalised as the overwrite mode for the NFC chip has been locked.

2 CONFORMANCE CLAIM

The ST and TOE are conformant to version 3.1 (REV 5) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 5), April 2017.
- **Part 3 conformant, EAL1.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 5), April 2017.
- No conformance to a Protection Profile is claimed.

3 SECURITY OBJECTIVES

3.1 Security objectives for the Environment

Table 3: Security Objectives for the Environment

IDENTIFIER	OBJECTIVE STATEMENTS
OE.INSTALL	The TOE shall be personalised, configured, delivered and set up in accordance with installation procedures defined in the guidance documentation.
OE.CLOUD	The AWS cloud platform are continuously hardened by AWS and monitored by TOE Developer to counter the perceived threats. The TOE Web App are being hardened through the AWS security protection enables as recommended by AWS includes establish a secure configuration to the OS, configure OS audit logs, configure proper OS authentication and permission, and ensure legacy services are not enabled.

4 Extended Components Definition

No extended components have been defined for this ST.

5 SECURITY REQUIREMENTS

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows **[assignment].**
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows ***[selection]*****.**
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded and underlined text, for <u>**additions**</u>, and strike-through, for ~~deletions~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Security functional requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Table 4: SFRs

Identifier	Title
FIA: Identification and authentication	
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT: Security management	
FMT_MTD.1	Management of TSF data

Identifier	Title
FMT_SMF.1	Specification of management function
FMT_SMR.1	Security roles
FPT: Protection of TSF	
FPT_FLS.1	Failure with preservation of secure state
FRU: Resource utilisation	
FRU_FLT.1	Degraded fault tolerance
FTA: TOE access	
FTA_SSL.4	User-initiated termination
FTA_TSE.1	TOE session establishment
FTP: Trusted path/channels	
FTP_ITC.1	Inter-TSF trusted channel

5.2.2 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment:** **a. TOE User: username (email address), password and unique link embedded inside the NFC chip and QR code; and** **b. TOE User Admin: username (email address) and password].**
Notes:	Note that, the QR Code is not part of the TOE scope of evaluation. Nonetheless, the SFR assignment declared on the QR Code as one of the component that are managed by the TOE operations and stored securely as one of TOE User data as in attributes related to the TOE User.

5.2.3 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Notes:	None.

5.2.4 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Notes:	None.

5.2.5 FMT_MTD.1 Management of TSF Data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to ***[selection: modify, delete, [assignment: create]]*** the **[assignment: TOE User personalised data at TOE Web App User Profile]** to **[assignment: TOE User Admin, TOE User]**.
Notes:	In the default profile page, the delete function are not available except for additional profile page created by TOE User. The delete function (button) will be available if there are more than one profile page created.

5.2.6 FMT_SMF.1 Specification of management function

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[assignment:** **a. TOE User Admin: managing all TOE User account (create, modify and remove), manage (modify) unique link to the TOE User Profile, and manage (assign and delete) TOE NFC Card to the TOE User Profile.** **b. TOE User: manage (edit) unique link to the TOE User Profile.** **].**
Notes:	None.

5.2.7 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FMT_SMR.1.1	The TSF shall maintain the roles **[assignment: TOE User and TOE User Admin**].

FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Notes:	None.

5.2.8 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **[assignment: fail to inject new link or code (triggered overwrite protocol on NFC chip) into the protected TOE NFC Card, locked personalised chip as in locked write protocol]**.
Notes:	None.

5.2.9 FRU_FLT.1 Degraded fault tolerance

Hierarchical to:	No other components.
Dependencies:	FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.1.1	The TSF shall ensure the operation of **[assignment: read on NFC chip of TOE NFC Card]** when the following failures occur: **[assignment: error code prompted "fail to write"]**.
Notes:	The method of injection unvalidated code (malicious code or unknown code) to the NFC chip are being explained in this SFR. Indeed the action are being performed by NFC reader in the mobile phone, in which the action performed by the NFC reader may lead to intention of code injection that this SFR claimed to prevent this action from happening. Thus, this SFR claimed that the TOE (data and configuration reside in the NFC card) are being protected from code injection by providing error of "fail to write" using the method of disable of write protocol personalised by the TOE Developer on the NFC card.

5.2.10 FTA_SSL.4 User-initiated termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.
Notes:	This SFR been declared for this ST with the justification that the TOE User Admin or TOE User should be aware that a session may continue after the terminated his/her activity, for example, on hold data been updated by TOE User without been save (clicked button "Save"). This requirement would allow the user to terminate this background activity without regard to the status of the activity. In that sense that the TOE User or TOE User Admin may terminate the session upon clicking button logout and there were no changes made on the data/configuration if the button "Save" was not clicked. Somehow, this SFR able to provide protection for the TOE on possible data/configuration changes without proper validation.

5.2.11 FTA_TSE.1 TOE session establishment

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [**assignment: If there were no HTTPS connection enabled**].
Notes:	None.

5.2.12 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels

	and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit ***[selection: another trusted IT product]*** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for **[assignment: enabling HTTPS connection for:** **a. Opening the unique URL embedded in the NFC and QR code; and** **b. Accessing TOE Web App]**.
Notes:	Here in this SFR declared as trusted IT products which are: internet browser mobile application, desktop PC internet browser, QR Code scanner and NFC reader, that will be communicating with the TOE upon request using the unique link stored in the NFC chip. Note that, the QR Code is not part of the TOE scope of evaluation. Nonetheless, the SFR assignment declared on the QR Code as one of the component that are managed by the TOE operations and stored securely as one of TOE User data as in attributes related to the TOE User.

5.3 TOE Security assurance requirements

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

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

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

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

Table 5: SARs

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing – conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

6 TOE SUMMARY SPECIFICATION

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE actually implements the claimed security functional requirements.

The TOE security functions include the following:

a. **Identification and Authentication**

b. **Security Management**

c. **Secure Access**

d. **NFC Data Tampering Protection**

6.2 Identification and Authentication

The TOE provides the capability to enforce an access control policy ensuring that only authorized TOE User Admin and TOE User are able to access the TOE Web App via any forms of internet browser using the registered username (email address) and password.

The TOE possesses the capability to mandate all TOE User to input their registered credentials, which are username (email address) and password, for accessing the personalized TOE Web App developed for them. Once the user has been successfully identified and authenticated, they gain access to their individual Web App page.

The unique link embedded in the NFC Chip in the TOE NFC Card belongs to individual TOE User. Each TOE NFC Card is associated with individual TOE User Profile.

Note that, the QR code, QR code scanner, NFC reader and mobile phone are not part of TOE scope of evaluation.

Security Functional Requirements: FIA_ATD.1, FIA_UAU.2, FIA_UID.2 and FMT_SMR.1.

6.3 Security Management

TOE incorporates management functions overseeing the overall operations, TOE User management, and TOE configuration. This ensures that all TOE User can access their accounts, and individuals with access to the link via the TOE NFC Card or QR code can view it upon scanning. Plus as for the TOE User Admin, able to access their management functions related to the TOE, management of TOE User and subscribed TOE NFC Card (accessible for TOE User Admin).

As for the TOE User, their access is from the perspectives of managing their own information, content and credentials as registered TOE User of the TOE Web App specifically TOE Web App User Profile.

The TOE Developer manage the TOE operations, and TOE Configuration to ensure the smooth operations of the TOE, plus ensuring all the data reside in the TOE management are being protected.

Aside of that matter, the TOE User Admin are the authorised representative of the TOE User by their organisation to manage all TOE User accounts, manage TOE User profile and assignment of the TOE NFC Card to the TOE User. The creation of each TOE User profile will generate a unique URL link that will be personalised to the TOE NFC Card.

TOE Developer is responsible in managing the TOE User Admin accounts, subscription of the client/customer/subscriber and assignment of quantity of TOE NFC Car. However it is out of evaluation scope. In the aspects of TOE User Management and assignment of TOE NFC Card to the TOE User, only TOE User Admin is applicable to perform such management functions. TOE User, acting as custodians of the TOE NFC Card can only access their TOE Web App User Profile with authorization, enabling them to update their own data, content, information, and credentials.

Security Functional Requirements: FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1.

6.4 Secure Access

TOE ensures secure access through the utilization of HTTPS enabled by AWS security protection mechanisms. This guarantees the secure protection of all data transmitted between the TOE Web App and any internet browser(s) on mobile phones or other platforms. TOE Web App are safeguarded by HTTPS protocols and possible data/configuration changes made on the TOE without proper validation by TOE User Admin and TOE User.

With the link read by the NFC reader or scanner QR Code via camera of the mobile device, the link shall be disclosed to the internet browser (mobile or desktop) to view the TOE Web App User Profile that contained all the TOE User credentials such as phone number, address, links to social media, videos of advertisement related to their company etc. This page profile shall be enforced with HTTPS protocol secure connection.

HTTPS protocol secure connection shall be enforce upon accessing the TOE Web App and TOE Web App User Profile. Which are applicable for all the access by TOE User Admin and TOE User.

Additionally, any action taken by TOE User Admin and TOE User, such as selecting the logout function, will automatically terminate the session, ensuring that any unsaved actions are not enforced on the TOE.

Security Functional Requirements: FTA_SSL.4, FTA_TSE.1 and FTP_ITC.1.

6.5 NFC Data Tampering Protection

The TOE Developer personalizes each TOE NFC Card according to the user's specifications. Embedded within each personalized TOE NFC Card is a unique link that is securely protected, allowing permanent read-only access while disabling write access. This mechanism safeguards the NFC chip from being overwritten and prevents any attempts at data manipulation on the linked personalization stored within the NFC chip.

Note that, the TOE NFC Card that has been personalised for the TOE User can’t be re-personalised as the overwrite mode for the NFC chip has been locked. In the event of the attempt to write on the TOE NFC Card, there will be an error on the reader notification that triggered the error of “fail to write” using the method of disable of write protocol personalised on TOE NFC Card.

Security Functional Requirement: FPT_FLS.1 and FRU_FLT.1.