MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

First edition
2020-04-27

Guidelines for Securing MyKAD Enhanced Biometric Access (EBA) Ecosystem

Reference number:
MySEF-5-GUI-14-SC_MYKADECO-v1

REGISTERED OFFICE:

CyberSecurity Malaysia,
Level 7 Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia
Email: mysef_bd@cybersecurity.my

DISCLAIMER

This document is for informational purposes only. It represents the current thinking of CyberSecurity Malaysia on the security aspects of MyKAD EBA ecosystem. It does not establish any rights for any person and is not binding on CyberSecurity Malaysia or the public. The information appearing on this guideline is not intended to provide technical advice to any individual or entity. We urge you to consult with your own organization before taking any action based on information appearing on this guideline or any other documents to which it may be linked.

Contents **Page**

1 Introduction 1
1.1 Overview 1
1.2 Scope 1
1.3 Objectives 1
1.4 Intended audience 1

2 Terms, definitions, abbreviated terms and acronyms 1
2.1 Terms and definitions 1
2.2 Abbreviated terms and acronyms 5

3 MyKAD EBA 6
3.1 Background 6
3.2 What is EBA? 6
3.3 What is MyKAD EBA reader? 6
3.4 MyKAD EBA versus MyKAD 7

4 MyKAD EBA ecosystem 8
4.1 MyKAD EBA 9
4.1.1 Data type stored in MyKAD EBA cards 10
4.1.2 Detailed steps of MyKAD and MyKAD EBA process flow 10
4.2 MyKAD EBA reader 12
4.2.1 Types of MyKAD EBA reader 12
4.3 MyKAD EBA infrastructure 17
4.3.1 Personal computing environment 17
4.3.2 Client-server computing environment 18
4.3.3 Distributed computing environment 19
4.4 MyKAD EBA users 20
4.5 Comparison of MyKAD EBA process and deployment options 20

5 Secure operational environment of EBA ecosystem 21
5.1 Layer 1: MyKAD EBA security controls 22
5.2 Layer 2: MyKAD EBA reader security controls 22
5.3 Layer 3: MyKAD EBA infrastructure security controls 23
5.3.1 Security control - personal computing environment 23
5.3.2 Security control - client-server computing environment 24
5.3.3 Security control - distributed computing environment 25
5.3.4 Best practices for security controls 25
5.3.5 Location 27
5.4 Layer 4: MyKAD EBA users security controls 27
5.4.1 Security awareness 27

Bibliography 29

Acknowledgements 30

1 Introduction

1.1 Overview

This document describes the high-level architecture of Malaysian "Kad Akuan Diri" (MyKAD) Enhanced Biometric Access (EBA) and its ecosystem comprising of four (4) components namely: MyKAD EBA, MyKAD EBA reader, MyKAD EBA infrastructure and MyKAD EBA user. MyKAD is an identity card which is an asset for Malaysians as it is a proof of citizenship in Malaysia. It is also used to verify the card holder's identity in many aspects such as legal and financial transactions.

This document serves as a guidance to provide best practices in deploying a secure operational environment in MyKAD EBA ecosystem with security controls that need to be incorporated or addressed.

1.2 Scope

This document covers the security functions of the MyKAD EBA at a generic level that should be applicable to smart card readers with biometric protection capabilities distributed by National Registration Department (NRD).

1.3 Objectives

The objectives of this document are to provide guidance on the following:

a) The implementation of new security feature of MyKAD EBA;
b) The deployment of different types of MyKAD EBA reader and modes of EBA operation; and
c) Various security controls that can be implemented on the MyKAD EBA ecosystem.

1.4 Intended audience

This document provides guidance to the relevant stakeholders on the deployment of MyKAD EBA reader within its ecosystem including:

a) Public Sectors (e.g. Government Agencies)
b) Private Sectors (e.g. Financial Institution and Industries)

The intended audience can achieve appropriate security and trust levels by considering all the factors discussed in this document that can influence the overall security measures in their MyKAD EBA ecosystem.

2 Terms, definitions, abbreviated terms and acronyms

2.1 Terms and definitions

For the purposes of this document, the terms and definitions as the following apply:

2.1.1
application protocol data unit
The communication unit between a reader and a card. The structure of an APDU is defined by the ISO/IEC 7816 standards.

[ISO/IEC 7816-4:2013]

2.1.2
biometric reference
The plain biometric that is stored in the memory of computing environment or MyKAD EBA reader as a reference.

2.1.3
biometric thumbprint verification
Matching between captured biometric template on MyKAD EBA reader with stored biometric template inside MyKAD EBA.

2.1.4
biometric template
A digital reference of distinct characteristics that can be extracted from a biometric sample (minutiae).

2.1.5
command set document
A document that contains low-level programming instructions to read MyKAD.

[https://www.jpn.gov.my/en/informasimykad/mykad-command-set/]

2.1.6
common criteria
An international standard of guidelines and specifications developed for evaluating information security products, specifically to ensure an agreed-upon security standard for government deployments is met. It is a framework in which computer system users can specify their Security Functional Requirements (SFRs) and Security Functional Assurance Requirements (SARs) using Protection Profiles (PPs).

[ISO/IEC 15408:2017]

2.1.7
conformité européenne
Certification mark that indicates conformity with health, safety, and environmental protection standards for products sold within the European Economic Area (EEA) known as CE marking [1].

[European Commission, "CE marking." [Online]. Available: http://ec.europa.eu/growth/single-market/ce-marking/]

2.1.8
card holder
A MyKAD EBA holder.

Note 1: Can be a person who uses the service offered by the organization.

2.1.9
encrypted biometric
Biometric data that has been converted into a code to prevent unauthorized access.

2.1.10
enhanced biometric access
The additional security feature incorporated in the MyKAD by protecting the thumbprint biometric template through the process of mutual authentication, key agreement and secure messaging processes.

2.1.11
file control information
It is a part of ISO/IEC 7816 standards which defined as the string of data bytes available in response to a SELECT FILE command.

[ISO/IEC 7816-4:2013]

2.1.12
IT personnel
The staff who is employed by organization to perform and implement Information Technology (IT) related to MyKAD EBA.

2.1.13
JPN key
A set of byte number given by NRD and preprogramed in MyKAD EBA reader or SDK.

2.1.14
minutiae
Minutiae are defined as friction ridges characteristics that are used to individualise a thumbprint.

Note 1: Minutiae occur at points where a single friction ridge deviates from an uninterrupted flow. Deviation may take the form of ending division or immediate origination and termination.

[MS1960-1]

2.1.15
mutual authentication process
The process of biometric fingerprint matching securely through the cryptographic operations using PKI, between the MyKAD EBA reader and the biometric data inside the MyKAD EBA.

[Command Set and Guideline of EBA MyKAD Reading]

2.1.16
MyKAD
The Malaysian Kad Akuan Diri (MyKAD) is national identity card produced by National Registration Department (NRD) for Malaysian citizen.

Note 1: MyKAD term defined in this document is the previous version of MyKAD, which has the non MyKAD EBA specification.

2.1.17
MyKAD EBA
The new version of Malaysian Kad Akuan Diri (MyKAD) with additional security feature known as Enhanced Biometric Access (EBA).

2.1.18
MyKAD EBA ecosystem
The interconnected system of MyKAD EBA environment consist of MyKAD EBA, MyKAD EBA reader, MyKAD EBA infrastructure and MyKAD EBA users.

2.1.19
MyKAD EBA reader
Specific smart card reader that has the capabilities to read MyKAD and MyKAD EBA.

2.1.20
MyKAD key
A set of byte number given by NRD and preprogramed in MyKAD EBA.

2.1.21
offline mode
Mode of MyKAD EBA reader in the state of standalone (not connecting to computing environment) to perform authentication and verification of MyKAD EBA.

2.1.22
online mode
Mode of MyKAD EBA reader in the state of connecting to computing environment to perform authentication and verification of MyKAD EBA.

2.1.23
operator
The staff who is employed by the organization to deal with card holder's transaction related to MyKAD EBA.

2.1.24
organization
The organization who purchases or leases the MyKAD EBA reader solution. E.g. government agencies or financial institution.

2.1.25
plain biometric
Unencrypted thumbprint data. A format whereby the biometric template is ready for verification process.

2.1.26
public key infrastructure
A technology that uses a pair of keys for cryptographic operations to encrypt and sign data. One key is available to everyone (the public key) and the other is a secret (a private key).

2.1.27
sequence diagram
A sequence diagram shows object interactions arranged in time sequence.

Note 1: A sequence diagram depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

Note 2: Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

2.1.28
strong authentication
Any method of verifying the identity of a user or device that is intrinsically stringent enough to ensure the security of the system it protects by withstanding any attacks it is likely to encounter.

[https://www.stormshield.com/news/inside-networks-fighting-enemy]

2.1.29
technology security assurance
A national scheme initiated by CyberSecurity Malaysia (CSM) where ICT products are evaluated based on Mandatory Security Functional Requirements (MSFRs) developed by the Information Security Certification Body (ISCB).

[https://www.cybersecurity.my/en/our_services/mysef/main/detail/2658/index.html]

2.1.30
MyKAD EBA reader Type I
MyKAD EBA reader Type I performs EBA processes which includes mutual authentication, key agreement, secure messaging processes and cryptography keys to decrypt the biometric template on MyKAD EBA.

Note 1: The EBA processes are being performed in the firmware level reside in the reader's MicroController Unit (MCU).

[Protection Profile for Card Acceptance Device (CAD) With Biometric]

2.1.31
MyKAD EBA reader Type II
MyKAD EBA reader Type II performs EBA process includes mutual authentication, key agreement, secure messaging processes and cryptography keys to decrypt the biometric template on MyKAD EBA.

Note 1: The EBA processes are being performed by the Software Development Kit (SDK) installed in the computing environment such as Desktop PC.

[Protection Profile for Card Acceptance Device (CAD) With Biometric]

2.2 Abbreviated terms and acronyms

APDU	Application Protocol Data Unit
CC	Common Criteria
CE	Conformité Européenne
CNII	Critical National Information Infrastructure
CSM	CyberSecurity Malaysia
EBA	Enhanced Biometric Access
EEA	European Economic Area
FCC ID	Federal Communications Commission ID
FCI	File Control Information
HTTPS	Hyper Text Transfer Protocol Secure
ISCB	Information Security Certification Body
ISO	International Organisation for Standardization
LAN	Local Area Network
LCD	Liquid Crystal Display
MCU	MicroController Unit
MSFR	Mandatory Security Functional Requirement
MyKAD	Malaysia Kad Akuan Diri
MySEF	Malaysian Security Evaluation Facility

NRD	National Registration Department
PC/SC	Personal Computer Smart Card
PKI	Public Key Infrastructure
PP	Protection Profiles
SAR	Security Functional Assurance Requirement
SDK	Software Development Kit
SFR	Security Functional Requirements
TSA	Technology Security Assurance

3 MyKAD EBA

3.1 Background

Over the years, the MyKAD has changed forms, from a paper based laminated national identity card to a polycarbonate plastic card with an embedded microchip. As technology progresses, a single MyKAD is capable to host multiple applications such as identify information, driving license, passport, and health document [2].

The data in MyKAD particularly the biometric minutiae is considered as one of the critical national assets governed by Malaysian Government legislature. Despite MyKAD having several security features implemented, incidents still occurred. From 2017 to 2018, local news in East and West Coast of Malaysia have reported several cases of fake MyKAD syndicates [3][4]. These fake MyKAD were sold for thousands of Ringgits and used for jobs and loans applications [3][4].

In order to ensure the security features are robust to withstand tampering, manipulation and cloning by cyber attackers, NRD has taken the initiative to add EBA as another layer of security feature embedded on MyKAD.

In line with the new MyKAD EBA implementation and operations, MyKAD reader security functionalities should be enhanced in accordance to security features introduced in MyKAD EBA.

3.2 What is EBA?

EBA is an additional security feature which is embedded on MyKAD to secure the process of reading the biometric template on the reader or Software Development Kit (SDK). The retrieved biometric template is in the encrypted form. The EBA process includes three sub processes namely, mutual authentication, key agreement and secure messaging processes, and decryption of biometric template on MyKAD. With this new security feature, only authorized MyKAD EBA readers can read the biometric template.

3.3 What is MyKAD EBA reader?

MyKAD EBA reader is a smart card reader that is able to read MyKAD EBA and MyKAD produced by NRD. There are two types of MyKAD EBA reader, which are: Type I and Type II. Type I is able to operate in online and offline modes while Type II is able to operate only in online mode. MyKAD EBA reader has the capability to perform EBA process as discussed in Section 3.2. There are devices which offer two modes of operation, which are online and offline.

MyKAD EBA reader can access MyKAD that is designed with the chip storage capacities of 64KB and 80KB. The details of MyKAD EBA reader is further discussed in Section 4.2.

3.4 MyKAD EBA versus MyKAD

Figure 3.1 and Figure 3.2 illustrate the high-level process flow for accessing MyKAD and MyKAD EBA respectively. The difference between MyKAD EBA and MyKAD lies on the protection of biometric thumbprint template using the EBA security feature which consists of mutual authentication and encrypted biometric template as shown in Figure 3.2 (Step 3(2a),(2b) and (2c)).

In Figure 3.1, the process flow for MyKAD starts with the card holder is requested to insert his MyKAD in MyKAD EBA reader. The plain biometric template from MyKAD is extracted and stored in the memory of the computing environment or MyKAD EBA reader. The stored data is referred to as biometric reference. The card holder then needs to place his thumb on the thumbprint sensor of MyKAD EBA reader to capture the card holder's live biometric thumbprint image which is referred to as captured biometric image. This image is converted into captured biometric template, which will be compared to biometric reference for match and verification purposes. At the end, the verification status is displayed to the user.

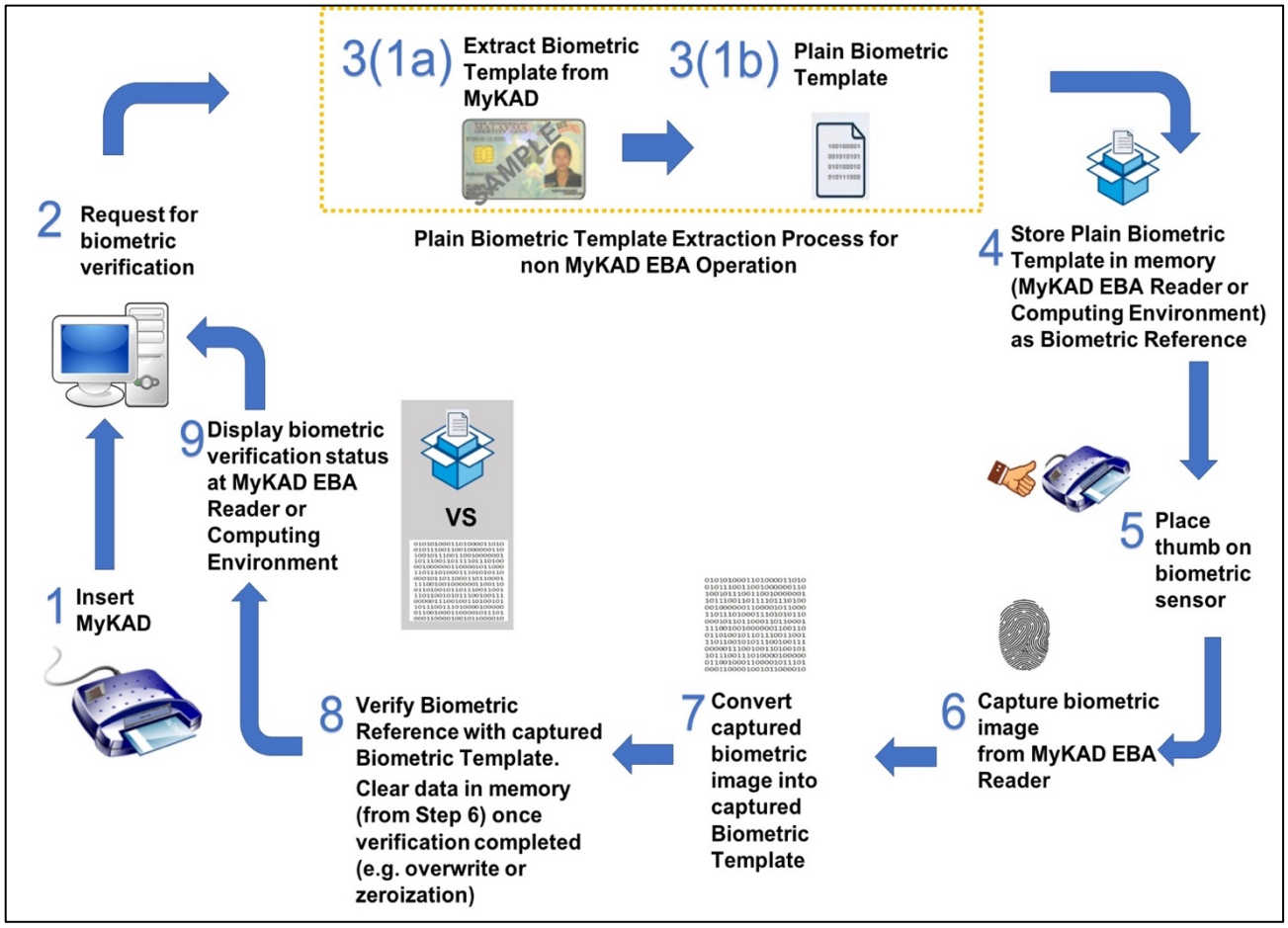

Figure 3.1 MyKAD Process Flow

Figure 3.2 shows the process flow of MyKAD EBA. The process is similar to MyKAD except that an additional logical security feature is added as shown in the dotted box (MyKAD EBA Operation). Step 3(2a) shows the process of mutual authentication between MyKAD EBA and MyKAD EBA reader. This is important to verify the genuineness of MyKAD EBA. In Step 3(2b), biometric template is extracted from MyKAD EBA in the encrypted form. Step 3(2c) shows the encrypted biometric template is decrypted into plain biometric template. The rest of the process is similar to MyKAD's process flow.

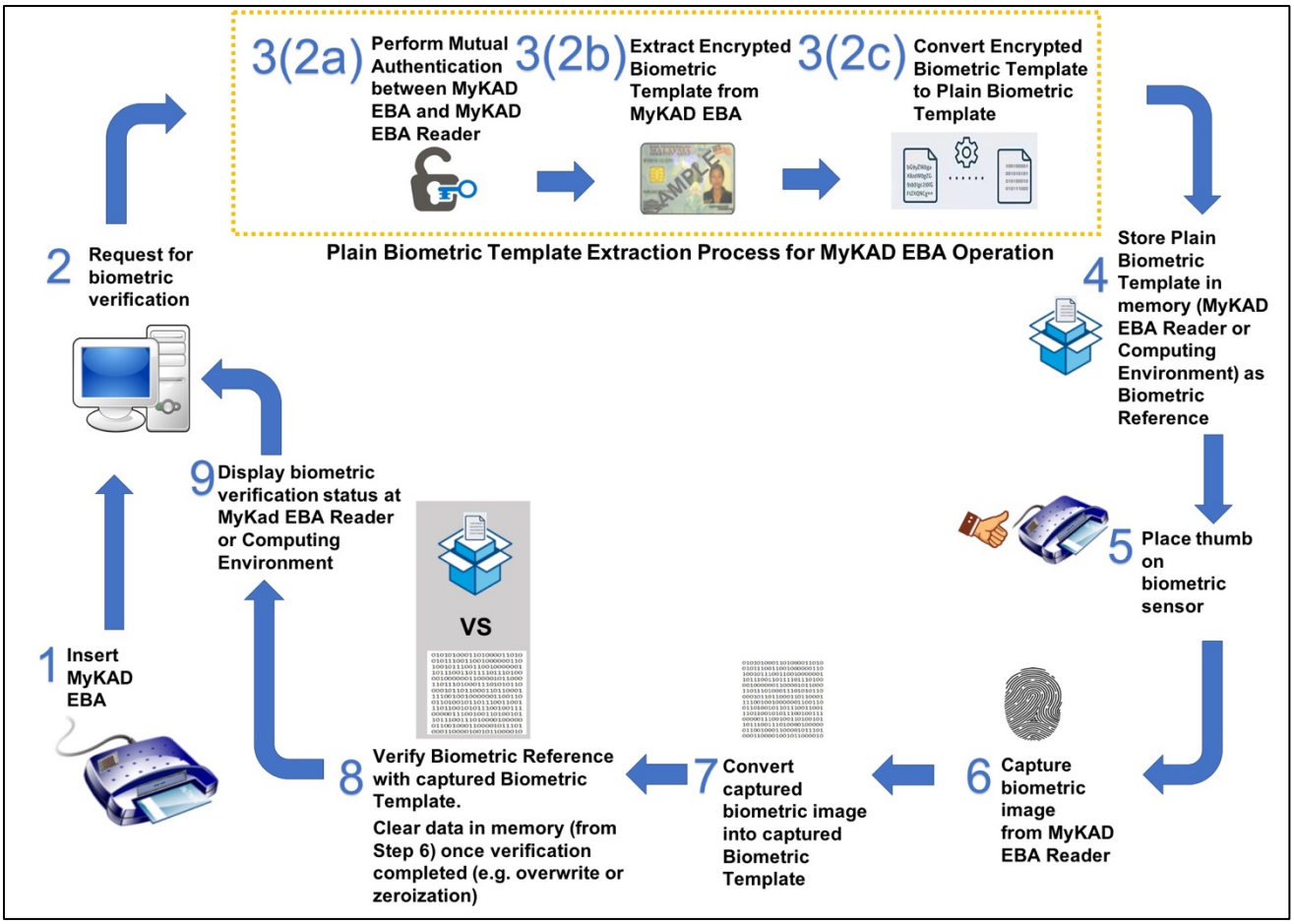

Figure 3.2 MyKAD EBA Process Flow

4 MyKAD EBA ecosystem

MyKAD EBA ecosystem is an interconnected network of various elements that combined to create a complete process of identification and authentication system using MyKAD EBA. Figure 4.1 illustrates the interconnection of the elements in each layer of MyKAD EBA ecosystem.

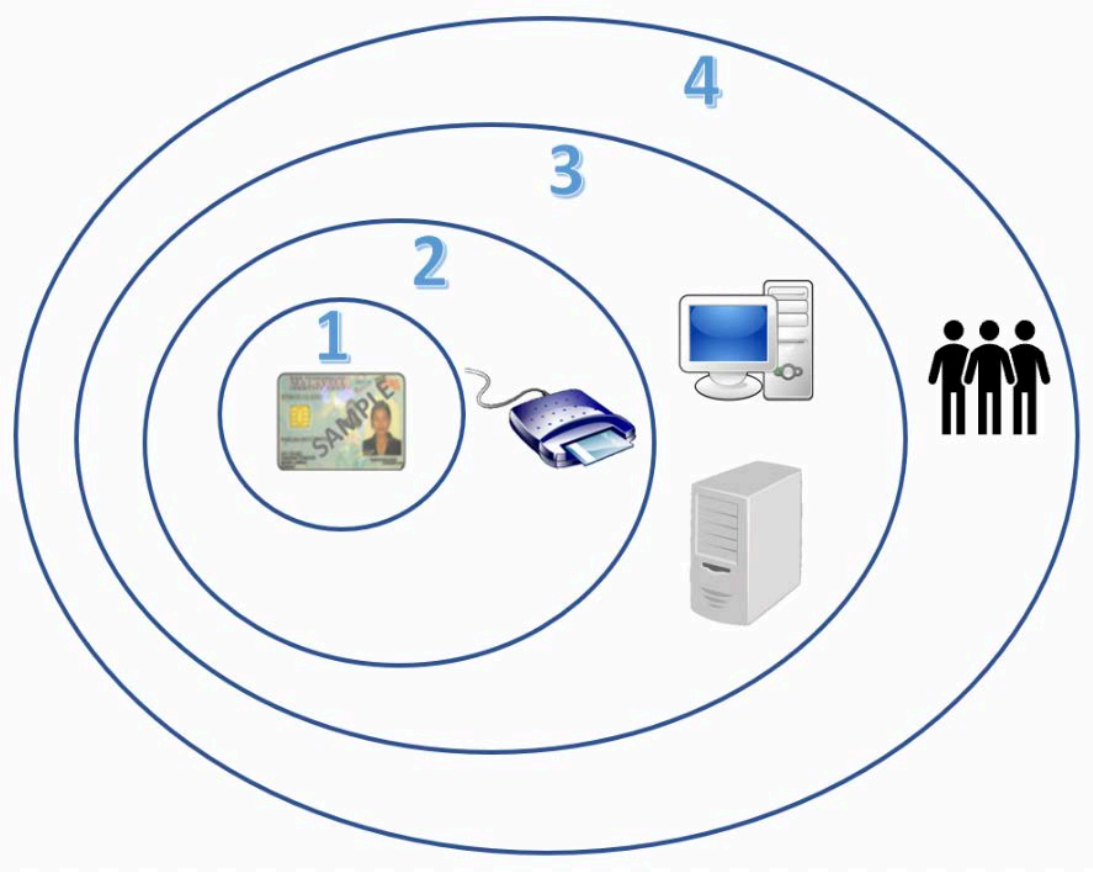

Figure 4.1 The MyKAD EBA ecosystem

The elements in the four layers are:

a) Layer 1: MyKAD EBA is the source of data;
b) Layer 2: MyKAD EBA reader enables the data exchange (biometric template) between the smart card (MyKAD EBA) and computing environment or defined as MyKAD EBA infrastructure. Typically, data exchange is in real time, however it depends on organization's implementation and standard of procedure.
c) Layer 3: MyKAD EBA infrastructure are resources such as desktop computer, server and network interface that processes the data e.g. biometric template; and
d) Layer 4: MyKAD EBA users who have different roles in MyKAD EBA ecosystem comprising of four categories which are organization, operator, IT personnel and card holder.

Organizations need to be familiarized with these layers as they are interdependent of each other. In this section, elements in each layer are discussed in detail. At the end, a summary of MyKAD EBA process and deployment options are provided to guide organizations in selecting MyKAD EBA reader and its related infrastructure that fit their needs.

4.1 MyKAD EBA

MyKAD EBA contains the data of MyKAD card holder. The format for all data are similar to MyKAD except for biometric thumbprint which is protected.

4.1.1 Data type stored in MyKAD EBA cards

Table 4.1 describes the data which are available in MyKAD EBA. Information stated are based on MS1960-2:2015 [5].

Table 4.1 Data Type in MyKAD

NO	DATA	DESCRIPTION
1.	Name	Name of card holder is stored in the chip and printed on surface (referred to General MultiPurpose Card (GMPC) name).
2.	ID Number	Identification number of card holder is stored in the chip and printed on surface.
3.	Photo	Photo of card holder is stored in the chip and printed on surface
4.	Old ID Number	Old identification number of card holder is stored in the chip and printed on surface. Note: This is only applicable to card holders who own the old version of identity card before the new format identification number was introduced.
5.	Address	Address of card holder is stored in the chip and printed on surface.
6.	Postcode	Postcode of card holder is stored in the chip and printed on surface.
7.	City	City of card holder stored in the chip and printed on surface.
8.	State	State of card holder stored in the chip and printed on surface.
9.	Citizenship Status	Card holder's citizenship status is stored in the chip and printed on surface
10.	Thumbprints	Card holder's thumbprints are stored in the chip with encrypted format
11.	Birth Date	Card holder's date of birth is stored in the chip
12.	Birthplace	Card holder's place of birth is stored in the chip
13.	Gender	Gender of card holder is stored in the chip and printed on surface
14.	Religion	Religion of card holder is stored in the chip and printed on surface (ISLAM only)
15.	Chip Serial Number	Card holder's chip serial number is stored in the chip and printed on surface
16.	Date Issued	Date card is issued to card holder is stored in the chip
17.	Race	Card holder's race is stored in the chip
18.	H or K Indicator	Indicator for card holder's place of birth is printed on surface (born in Sabah (H) or Sarawak (K) only)

4.1.2 Detailed steps of MyKAD and MyKAD EBA process flow

Figure 4.2 illustrates the detailed steps of MyKAD and MyKAD EBA process flows as discussed in Figure 3.1 and Figure 3.2.

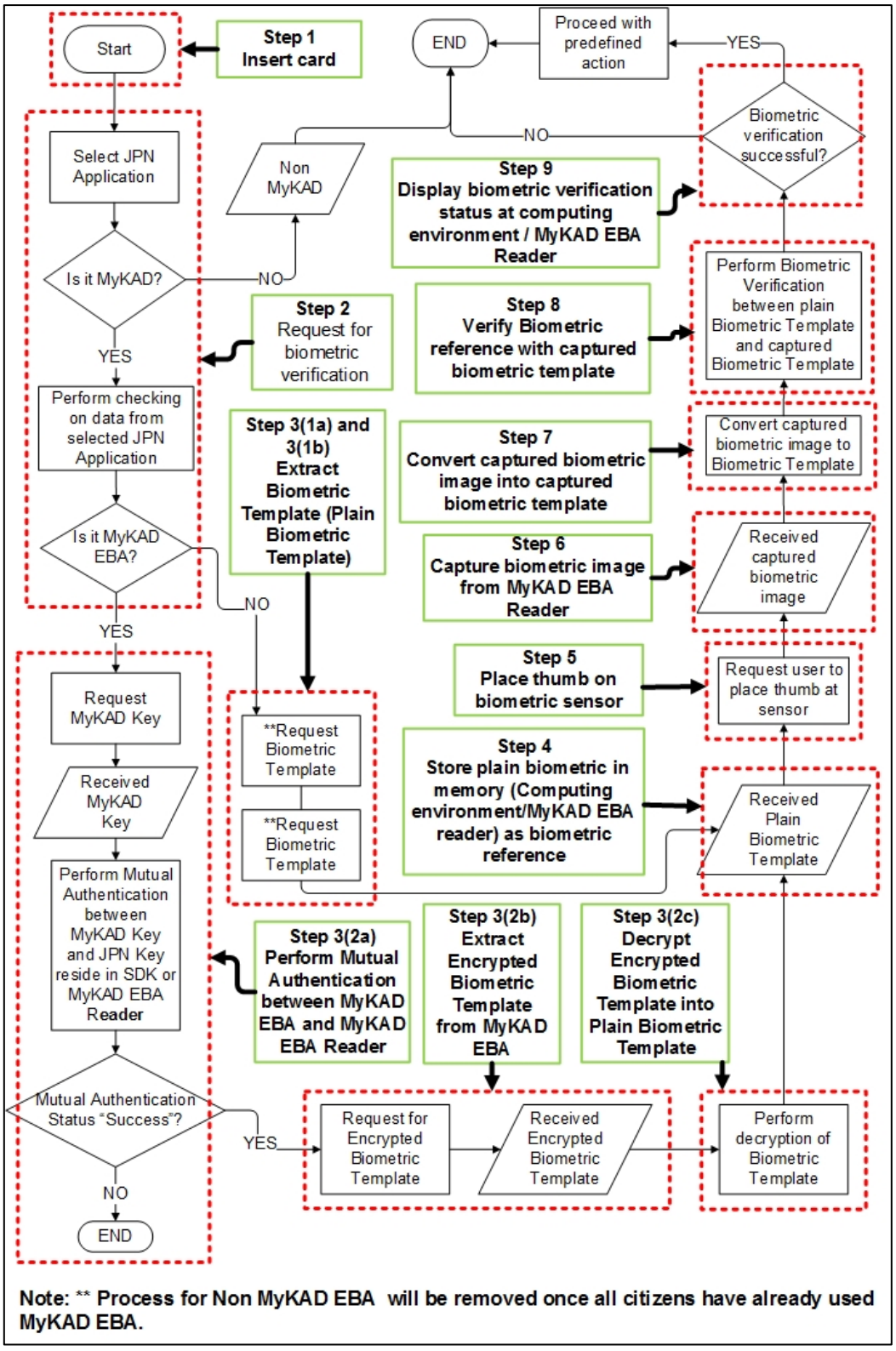

Figure 4.2 The Detailed Steps of MyKAD EBA and MyKAD Process Flow

The detailed steps of the process flow are as follows:

a) **Step 1:** The process starts when MyKAD is inserted in MyKAD EBA reader.
b) **Step 2:** The system requests for JPN Application. If the system receives a 'Success' status together with the string of File Control Information (FCI) data, it should proceed to check the FCI signature. If

status other than "Success" is returned, the system should conclude that it is a non MyKAD EBA operation and MyKAD EBA

c) **Step 3(1a) & 3(1b): plain biometric template extraction process for non MyKAD EBA operation** - The system will extract biometric template. The biometric template is in plain form.
d) **Step 3(2a), 3(2b) & 3(2c): plain biometric template extraction process for MyKAD EBA operation –**
    i) **3(2a)** Once the system detects the EBA FCI signature, the system will start the EBA operation by requesting for MyKAD Key. MyKAD Key should be genuine to pass the mutual authentication process. If it is not, mutual authentication will fail, and the process ends.
    ii) **3(2b)** System will request for the encrypted biometric template for the successful authentication process.
    iii) **3(2c)** The system performs decryption process to produce a plain biometric template. This template is matched against the card holder thumbprint.
e) **Step 4** to **Step 9** are similar to MyKAD EBA operations as described in Figure 3.1 and Figure 3.2.

4.2 MyKAD EBA reader

This section serves as a guidance and provides best practices for organizations in selecting MyKAD EBA reader.

Organizations can access the NRD and CSM official websites to check on the list of trusted manufacturers and model of readers which have received command set document from NRD before making decision of acquiring a new MyKAD EBA reader.

MyKAD EBA reader should function as specified in order to meet the business needs. Therefore, organizations need to assess the functional requirements and operational environment of the reader. It is highly recommended for organizations to ensure that the MyKAD EBA reader has gone through a third-party security evaluation.

It is recommended for organizations to acquire a certified MyKAD EBA reader which has gone through security evaluation such as Common Criteria (CC) and Technology Security Assurance (TSA). In the event that MyKAD EBA reader has been certified, organizations need to check the specific model numbers, including hardware and firmware versions to ensure that the model is valid according to the certificate.

Some of the security evaluation benefits of the certified MyKAD EBA reader are:

a) The reader meets the required security needs to ensure secured operation;
b) The reader is delivered with all features as requested;
c) It functions according to specifications as set out by the manufacturer;
d) It has an adequate guidance for it to be operated securely;
e) It has been thoroughly tested hence reducing the potential for exploitable vulnerabilities.

4.2.1 Types of MyKAD EBA reader

There are two types of MyKAD EBA reader; Type I and Type II reader. Type I reader performs EBA operation within the firmware of MyKAD EBA reader. For Type II reader, the EBA operation is performed on the host computing device such as Desktop Computer or Laptop Computer.

MyKAD EBA reader functions in two different modes, Offline mode and Online mode. In the Offline mode, MyKAD EBA reader operates as a Standalone System, whereas in the Online mode, MyKAD EBA reader can only be operated in a connected environment to complete the EBA operation.

Type I reader can operate in both modes; Offline and Online mode, while Type II reader can only operate in Online mode.

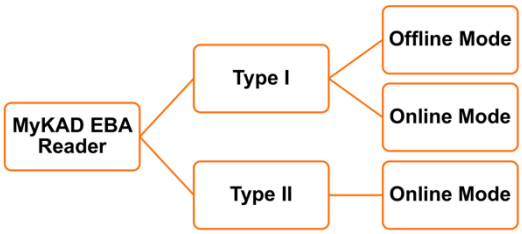

Figure 4.3 Types of MyKAD EBA reader

The mode of operations for each type of reader is as summarized in Figure 4.3.

Figure 4.4 and Figure 4.5 are examples of biometric verification sequence diagram for Type I, whereas, Figure 4.6 is an example for Type II.

The steps highlighted in the dotted boxes in Figure 4.4, Figure 4.5 and Figure 4.6 are the default biometric verification processes, where other steps can be changed based on manufacturer's design. Note that the processes shown are only for the main MyKAD EBA process. As for the detailed process, kindly refer to the command set document. The information that can be accessed includes name, address, identity card number, photograph, thumbprint minutiae, driving licence and passport [6].

4.2.1.1 Type I - Offline mode

Figure 4.4 shows the typical sequence diagram for MyKAD EBA reader Type I with Offline mode which the reader starts to operate when powered by battery.

The detailed process is as follows:

i) First, switch on MyKAD EBA reader to start the operation.
ii) Once turned on, the reader is triggered to initiate biometric verification function.
iii) Next, the reader will request the operator to select JPN Application for MyKAD EBA.
iv) MyKAD EBA will respond with the selection status; Successful or Unsuccessful.
v) Next, the reader will request for MyKAD Key from MyKAD EBA which is currently inserted in the reader's slot.
vi) MyKAD EBA will respond by sending MyKAD Key to the reader. The reader will decrypt MyKAD Key to produce plain key.
vii) The reader will proceed with the mutual authentication process, in which the necessary "handshake" is performed between the plain key and JPN Key as required.
viii) Next, the reader will request for the encrypted biometric template that is stored in MyKAD EBA.
ix) MyKAD EBA will respond to the reader by sending the encrypted biometric template.
x) This encrypted biometric template is then decrypted by the reader.
xi) After the reader successfully decrypts the encrypted biometric template, the reader will request the card holder to place his thumb on the reader's sensor. The operator is being notified using certain indicator such as an appearance of red light or audible sound.
xii) Next, the reader will perform biometric thumbprint verification process. In this process, the captured biometric image of the thumbprint will be matched against the decrypted biometric template.

xiii) Finally, the status of the verification process will be displayed on the reader's LCD.

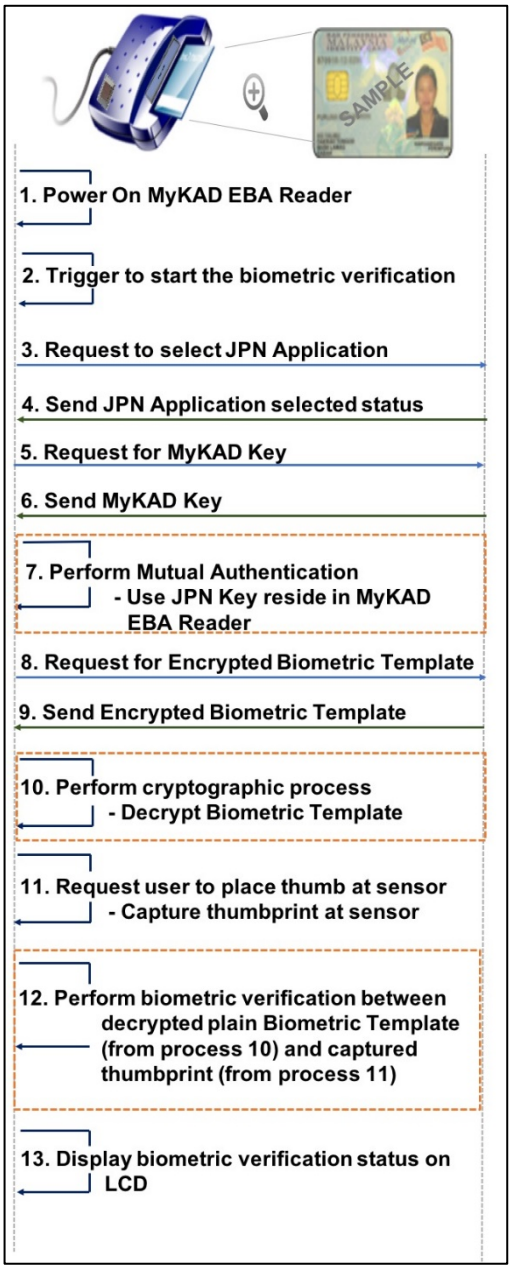

Figure 4.4 Type I - Offline Mode

4.2.1.2 Type I - Online mode

Figure 4.5 illustrates a typical sequence diagram for Type I reader under the Online mode. The application is developed and integrated with the reader through SDK.

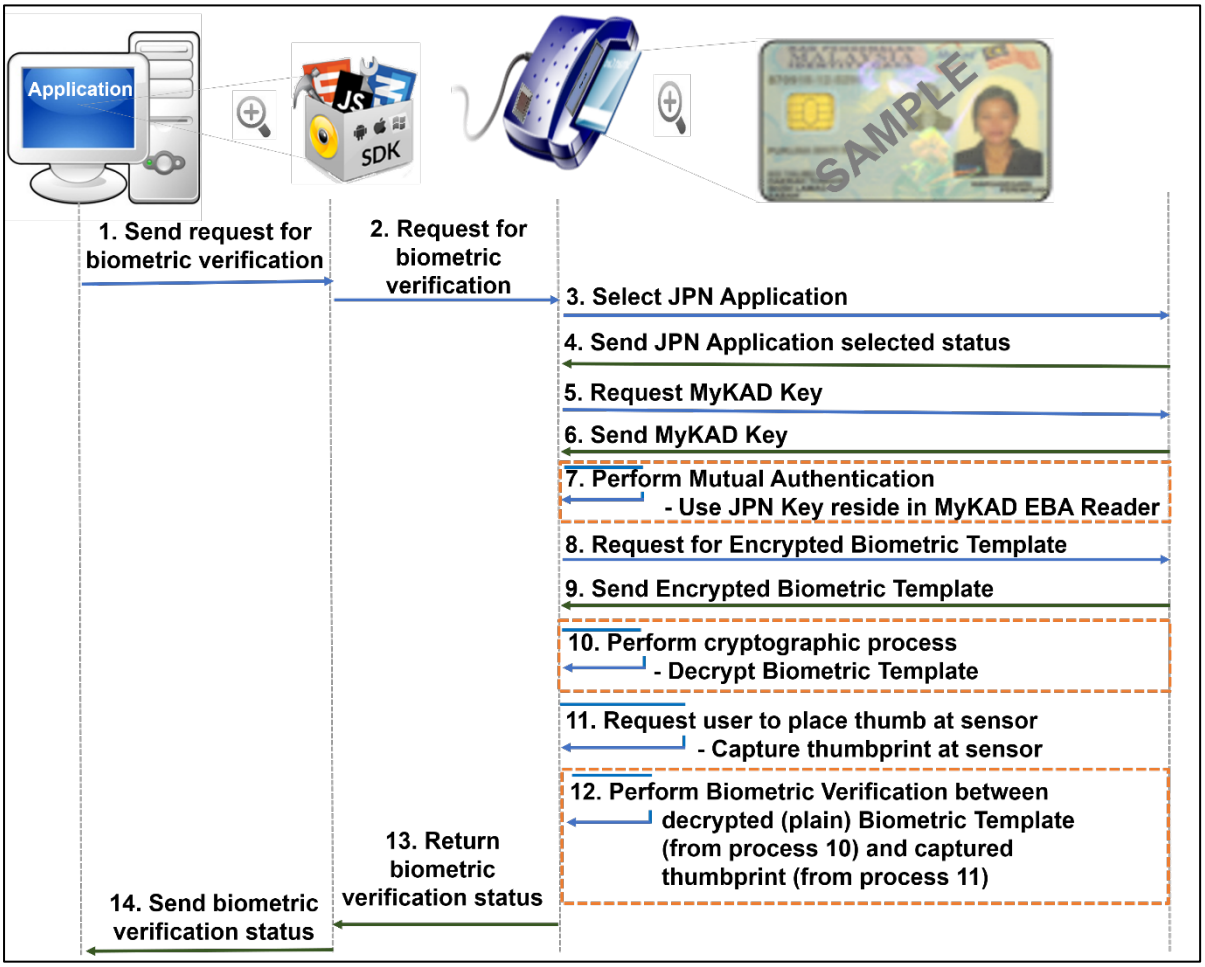

Figure 4.5 Type I - Online Mode

The detailed steps for MyKAD EBA reader Type I under the Online mode are as follows:

i) The process begins when the application is triggered as the operator clicks the biometric verification start button.
ii) The request will be transferred to the function which performs the verification process inside the SDK.
iii) Then, the reader will request to select JPN Application from MyKAD EBA.
iv) MyKAD EBA will respond back with status and data.
v) Next, the reader will request for MyKAD Key from MyKAD EBA which is currently inserted in the reader's slot.
vi) MyKAD EBA will respond back and send MyKAD Key to the reader.
vii) The reader will perform mutual authentication process after MyKAD Key has been received. mutual authentication process will be performed using the JPN Key that resides in the reader with the received MyKAD Key.
viii) If this process is successful, the reader will only be able to request for biometric template from MyKAD EBA.
ix) MyKAD EBA will respond to the reader by sending an encrypted biometric data.
x) Then, the reader will decrypt the received encrypted biometric template.
xi) After the reader successfully decrypts the encrypted biometric template, it will give signal, e.g. red light appears, for the card holder to place his thumb on the reader sensor.
xii) The captured data from the thumbprint is matched against the decrypted biometric template.
xiii) The status of verification process is sent to SDK.
xiv) The SDK then updates the status to the application according to the application requests process.

4.2.1.3 Type II - Online mode

Figure 4.6 Type II – Online mode shows a typical sequence diagram for Type II reader under the Online mode. The developer will develop an application and integrate it with the reader through SDK.

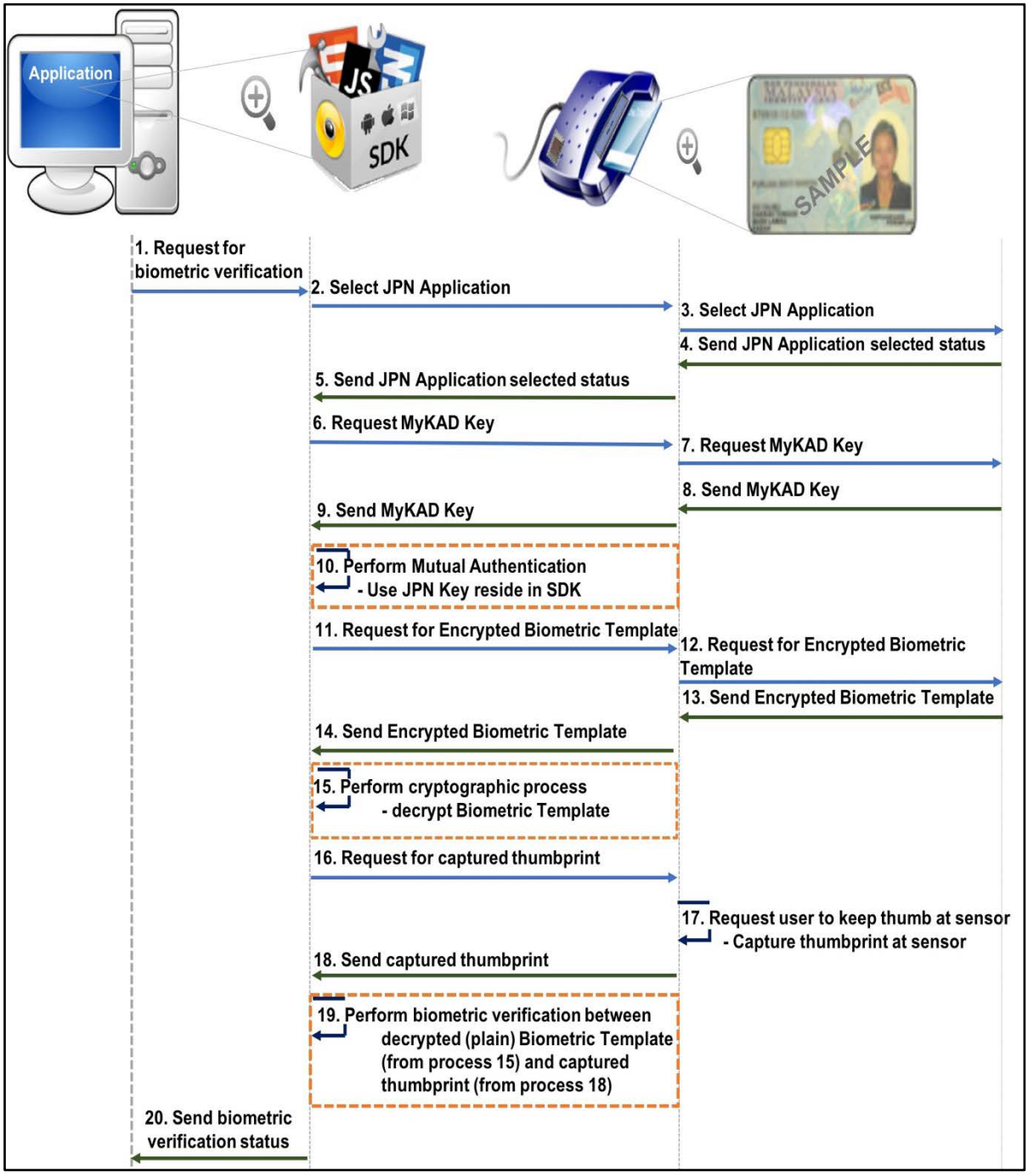

Figure 4.6 Type II – Online Mode

The processes involved are detailed as follows:

i) The application is triggered when the operator clicks on the biometric verification start button. The request will be transferred to the function which will perform the verification process inside the SDK.

ii) The SDK will request the reader to select JPN Application.
iii) The reader will then send the request to MyKAD EBA.
iv) MyKAD EBA will respond back to the reader with the selected status and data.
v) The reader will pass the selected status and data to the SDK.
vi) Next, the SDK will request MyKAD Key from the reader.
vii) The reader will pass on the request to MyKAD EBA which is currently inserted in the reader slot.
viii) MyKAD EBA will respond with the requested key.
ix) The reader will then send the received MyKAD Key to SDK.
x) Next, mutual authentication process will be performed by the SDK using the JPN Key that resides in the SDK with the received MyKAD Key.
xi) If this process is successful, the SDK will request for biometric template from the reader.
xii) The reader will send the request to MyKAD EBA.
xiii) MyKAD EBA will respond by sending the encrypted biometric data to the reader.
xiv) The reader will then send encrypted biometric data to SDK.
xv) Next, the SDK will decrypt the received encrypted biometric template for the next process.
xvi) After the SDK successfully decrypts the biometric template, the reader will produce a signal, e.g. red light, for the card holder to place his thumb on the reader sensor.
xvii) The reader will send the captured thumbprint data to the SDK.
xviii) The SDK will then perform biometric verification process between the decrypted biometric template and the captured thumbprint data.
xix) The verification status is sent to the SDK.
xx) The SDK will then update the status to the application according to the application requests process.

4.3 MyKAD EBA infrastructure

MyKAD EBA infrastructure consists of a set of information technology (IT) components that are the foundation of an IT service; typically, physical components (computer and networking hardware and facilities), but also various software and network components.

The service runs depending on MyKAD EBA organization, the infrastructure of a computing environment may vary. For example, the computing environment usage is the installed application (software) that initiates the biometric verification processes, displays outputs of MyKAD reading and configuration of MyKAD EBA reader.

There are three types of computing environments in the MyKAD EBA ecosystems which are:

a) Personal Computing Environment (Refer to Figure 4.7);
b) Client-Server Computing Environment (Refer to Figure 4.8); and
c) Distributed Computing Environment (Refer to Figure 4.9).

4.3.1 Personal computing environment

In this environment, the MyKAD application resides in the desktop and the application shall be executed within the same desktop. It does not need to access Local Area Network (LAN) in order to access the MyKAD application.

Figure 4.7 shows an example of the implementation of personal computing environment for MyKAD EBA reader.

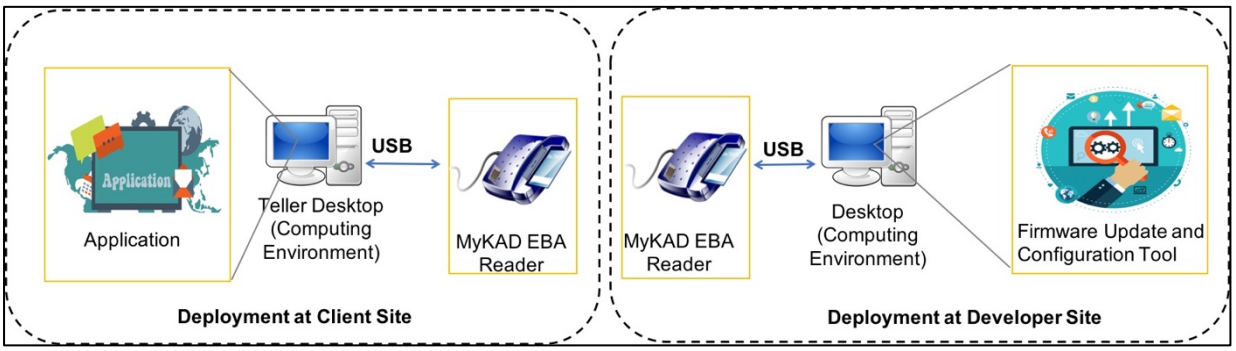

Figure 4.7 Personal Computing Environment

Example of implementation: At client site (registration counter at government office), the software application reading MyKAD EBA is installed within the same machine together with the reader attached to it. The implementation does not involve any network functionality. If the reader requires a firmware update or new configuration setting, the reader need to be sent back to the developer site.

4.3.2 Client-server computing environment

The client-server environment consists of two machines; a client machine and a server machine. Both machines will exchange the information through an application. The client machine is a normal computer such as PC, Tablet, mobile devices and etc. The server is capable of storing huge data and manages huge amount of file, emails, and etc.

In this environment, the client requests data and the server then provides the data to the client. In the client-server environment, the communication between the client and the server is performed using Hyper Text Transfer Protocol Secure (HTTPS).

Figure 4.8 shows an example of the implementation of the client-server computing environment for MyKAD EBA reader.

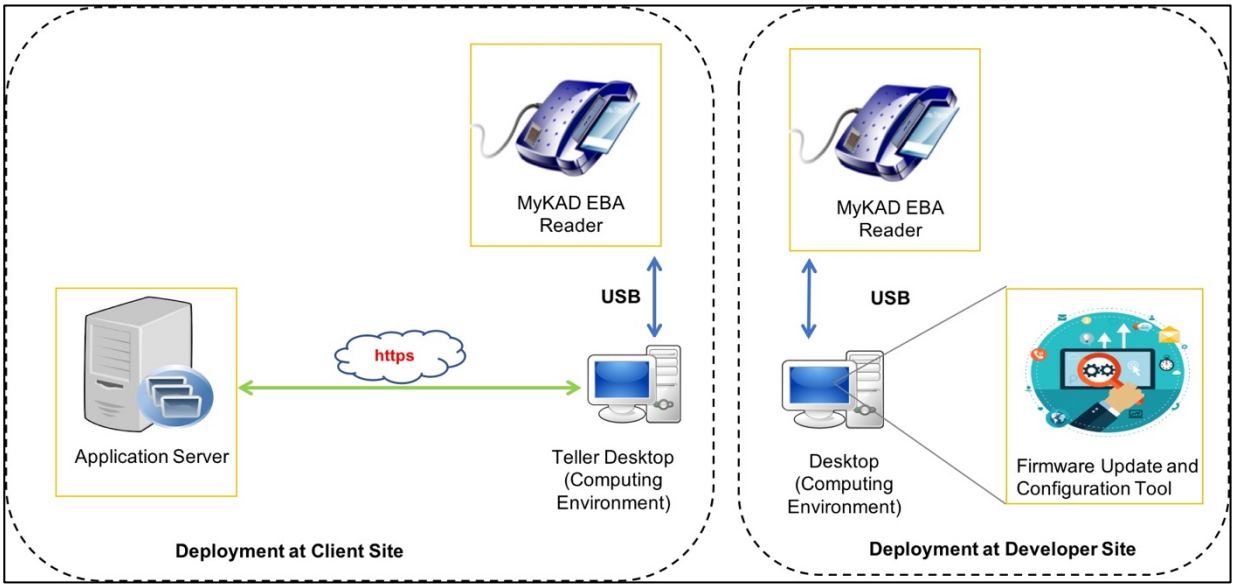

Figure 4.8 Client-Server Computing Environment

Example of implementation: The desktop (connected to MyKAD EBA reader) accesses the web application through a network (Local Area Network or Wide Area Network) to execute reading MyKAD. However, if the reader requires a firmware update or new configuration setting, the reader still needs to be sent back to the developer site.

4.3.3 Distributed computing environment

In the distributed computing environment, the full functionality of the software is not in a single computer but is distributed to several computers. These computers are connected with each other through the network to perform the full task. In distributed computing environment, the data is distributed to different systems and logically tied to each other.

Figure 4.9 shows an example of the implementation of the distributed computing environment for MyKAD EBA reader.

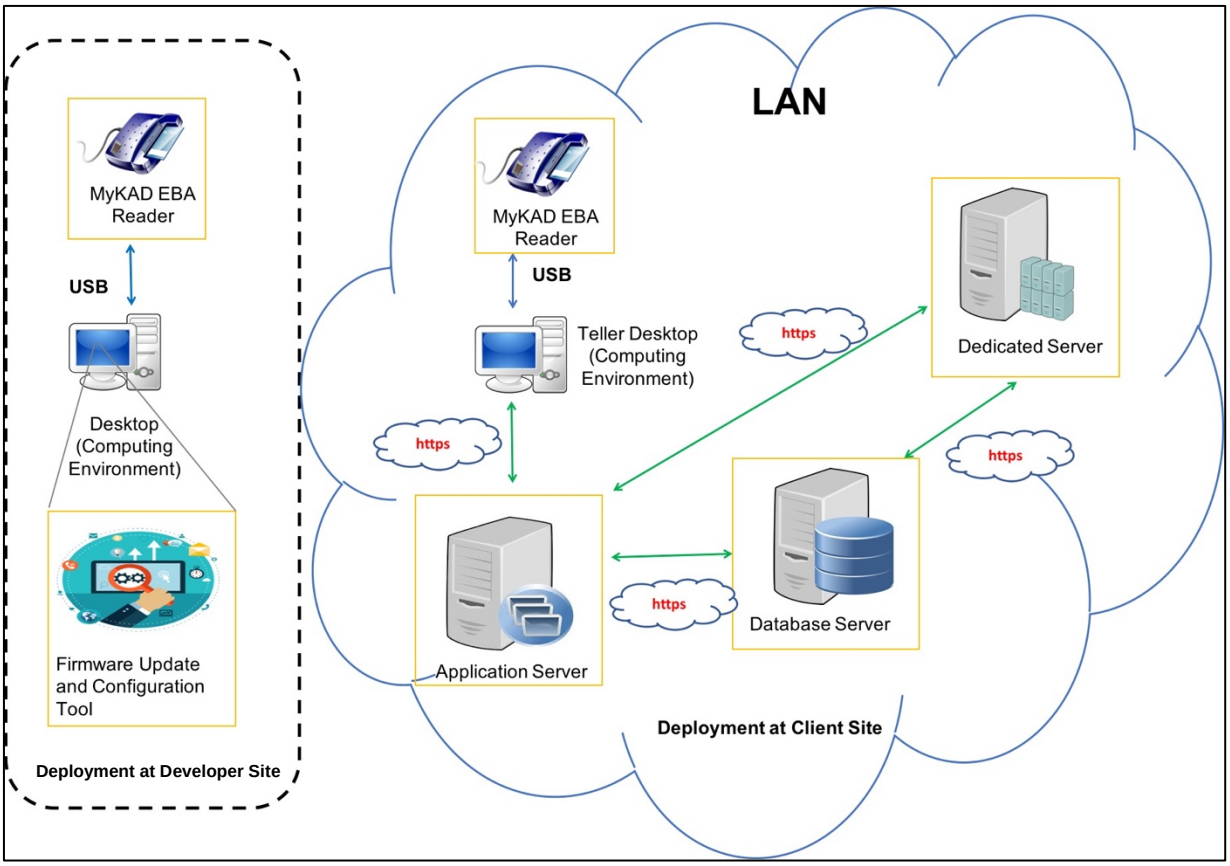

Figure 4.9 Distributed Computing Environment

Example of implementation: A dedicated server is implemented to control all the distributed computing environment. The desktop connected with MyKAD EBA reader, requests to read MyKAD data through application that can be assessed from the dedicated server. Regardless of the kind of data requested, the dedicated server will distribute the task to other servers (Application Server and Database) and return the data to the teller's desktop. However, similar to Personal Computing and Client Server environment, if the reader requires a firmware update or new configuration setting, the reader still needs to be sent back to the developer site.

In any networking infrastructure, network devices such as servers are vulnerable to security threats. Example of these threats include [9]:

a) Brute Force Attack – a brute force attack refers to an attack that uses software to access a server. The attacker will typically try all possible combination of users' password to break into the server.
b) Cross-Site Scripting – cross-site scripting is a technique used by an attacker to inject code in a server-side script. The aim is to execute malicious client-site scripts and gather sensitive data. Application servers are typically vulnerable to this threat.
c) SQL Injection – Database is vulnerable to SQL injection, in which the attackers will attempt to insert malicious code into strings that are passed to the SQL server, parsed and executed.

4.4 MyKAD EBA users

Users are the party that have different roles in MyKAD EBA ecosystem comprising of four categories which are organization, operator, IT personnel and card holder. Figure 4.10 shows an example of different roles of MyKAD EBA users in a financial institution.

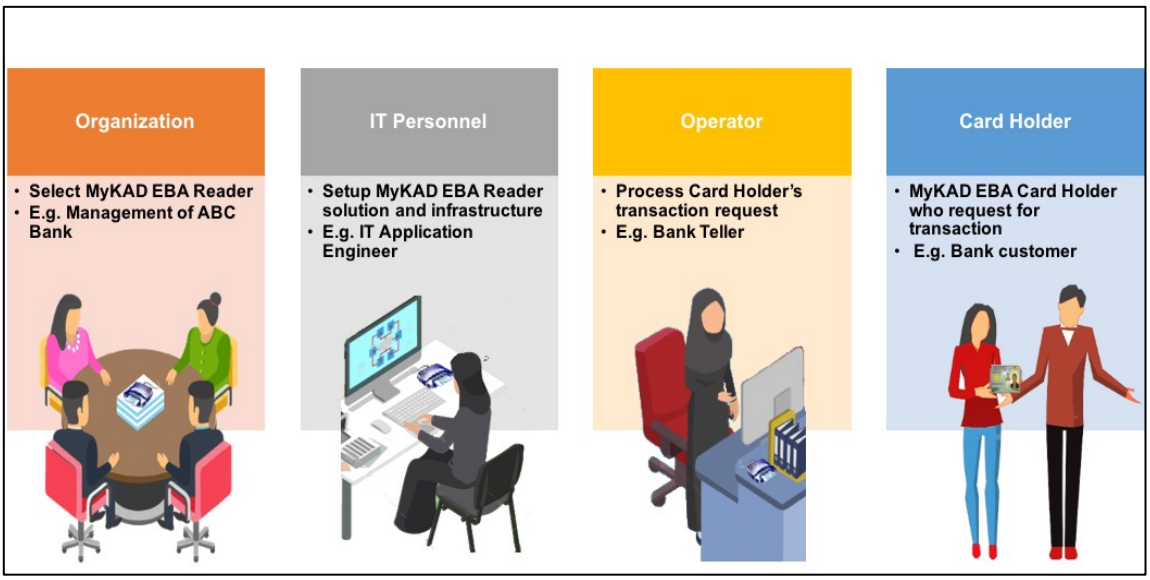

Figure 4.10 Example of MyKAD EBA Users in a Financial Institution

4.5 Comparison of MyKAD EBA process and deployment options

Table 4.2 shows the comparison of MyKAD EBA process for Type I and Type II.

Deployment options for different types of MyKAD EBA reader are given in Table 4.3. This information serves as a guidance for organizations to compare MyKAD reader based on their organizational needs.

Table 4.2 Comparison of MyKAD EBA process

NO	PROCESS	TYPE I		TYPE II
		OFFLINE	ONLINE	ONLINE
1.	EBA Operation	Hardcoded in the MyKAD EBA reader's firmware	i. Hardcoded in the MyKAD EBA reader's firmware ii. Only biometric verification status is passed back to SDK	EBA operation is hardcoded in MyKAD EBA reader's SDK

2.	Storage location of JPN Key	Firmware	Firmware	SDK
3.	Processing and storage of MyKAD sensitive data	Firmware	Firmware	SDK
4.	Processing and storage of thumbprint template	Firmware	Firmware	SDK

Table 4.3 Comparison of MyKAD EBA deployment options

NO	PROCESS	TYPE I		TYPE II
		OFFLINE	ONLINE	ONLINE
1.	Location	Remote/ Outskirts area	Over the counter/Kiosk	Over the counter
2.	Mobility	Can be operated by power source (power bank or internal battery)	Needs computing environment to operate	Needs computing environment to operate
3.	Application Integration	Application integration is not required	As all EBA operation is performed in the firmware of MyKAD EBA reader, minimal efforts are required for integration	EBA operation is performed in SDK, therefore higher efforts for integration

5 Secure operational environment of EBA ecosystem

This section serves as a guidance that provide best practices to ensure secure operational environment for MyKAD EBA ecosystem. Each element in the MyKAD EBA ecosystem layers should be protected as threats and vulnerabilities can come from different sources. There is a systematic way to mitigate the threats and vulnerabilities. Figure 5.1 shows the different type of layers that need to be protected:

a) Layer 1: MyKAD EBA security controls;
b) Layer 2: MyKAD EBA reader security controls;
c) Layer 3: MyKAD EBA infrastructure security controls (e.g. servers, application, network); and
d) Layer 4: MyKAD EBA users security controls which only apply to organizations, operators and IT personnel.

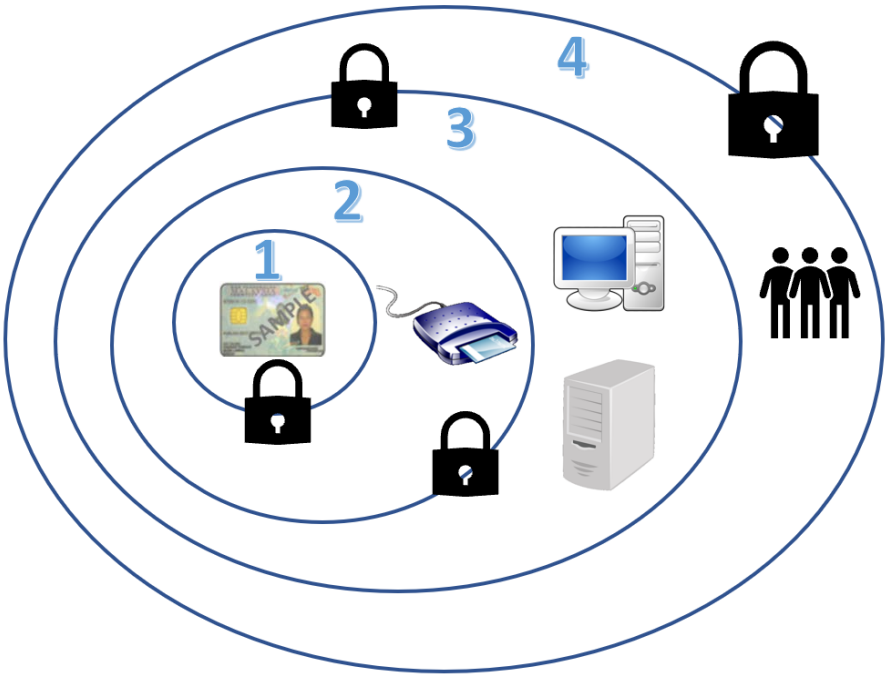

Figure 5.1 Protection at every layer in the ecosystem

It is recommended that organizations manage their security operation in accordance to the ISO/IEC 27001 Information Security Management Requirement which is a systematic approach to managing sensitive company information so that it remains secure [7]. It includes people, processes and IT systems or technologies by applying a risk management process in which the implementation guidance of security controls is based on ISO/IEC 27002 Code of practice for information security controls [8]. However, the discussion in the subsequent sub sections provide the basic security controls in each layer in the MyKAD EBA ecosystem.

5.1 Layer 1: MyKAD EBA security controls

MyKAD EBA has physical security features which is similar to MyKAD. Most of these security features can be observed through detailed inspection on MyKAD EBA. It is recommended for operators to inspect these features before proceeding with biometric verification process of the MyKAD EBA. For further details of the physical security features, it is recommended to refer to NRD website.

5.2 Layer 2: MyKAD EBA reader security controls

Figure 5.2 outlines the physical security features on MyKAD EBA reader. It is recommended for organizations to inspect these features before purchasing MyKAD EBA reader.

During implementation, IT personnel in charge of handling MyKAD EBA reader should ensure that there is no tampering on the reader's casing. There are two types of tamper protection implementation which are tamper evidence and tamper resistant. Tamper evidence is a tamper seal that provides visual evidence when tampering occurred. While tamper resistant is to prevent unauthorized opening of MyKAD EBA reader's case, examples security screws that holds the case tightly.

It is recommended for organizations to check whether MyKAD EBA reader has undergone certification process by authorized organization such as CE marking. Organizations also need to ensure manufacturer name, model and serial number stated on MyKAD EBA reader are correct.

It is also recommended for organizations to check whether MyKAD EBA reader has undergone security certification process acknowledged by the government of Malaysia such as Common Criteria (CC) and Technology Security Assurance (TSA).

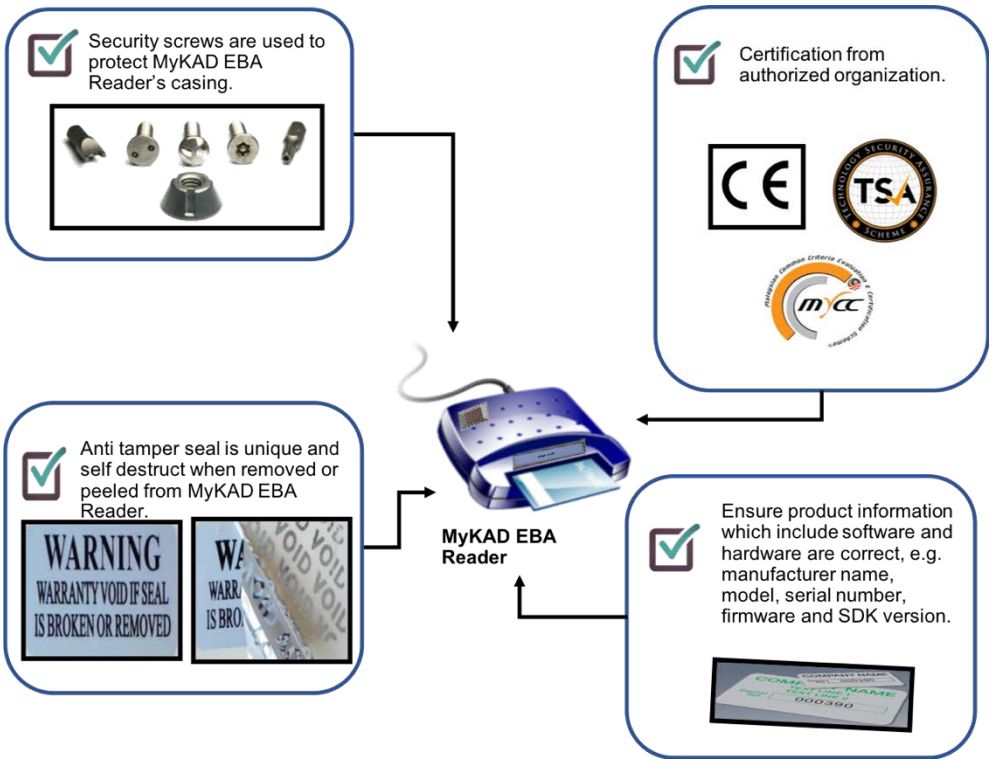

Figure 5.2 MyKAD EBA Reader Security Features

5.3 Layer 3: MyKAD EBA infrastructure security controls

In order to safeguard the infrastructure that surrounds the MyKAD EBA application, organization are encouraged to implement security controls in their computing environment to mitigate the threats such as:

a) External hackers, malicious individuals, cyber criminals;
b) Internal malicious individuals, internal user mistakes, human errors; or
c) Thief or intruder intending to cause physical damage or steal assets.

5.3.1 Security control - personal computing environment

Figure 5.3 describes an example of security control points that is recommended to be deployed in a personal computing environment.

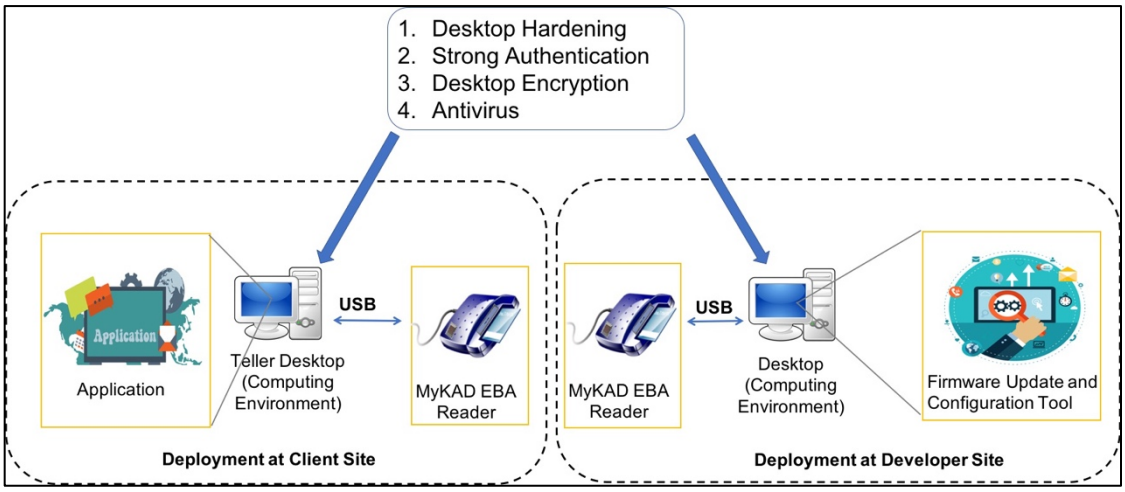

Figure 5.3 Security Control - Personal Computing Environment

The desktop hardening, strong authentication, desktop encryption and antivirus can be implemented in the application at the client's desktop. Occasionally, the firmware inside the MyKAD EBA readers need to be updated, therefore the same security controls for the client's desktop are also recommended to be implemented in Firmware Update and Configuration Tool at the developer's desktop.

5.3.2 Security control - client-server computing environment

Figure 5.4 describes the security control points that should be implemented in a client-server computing environment.

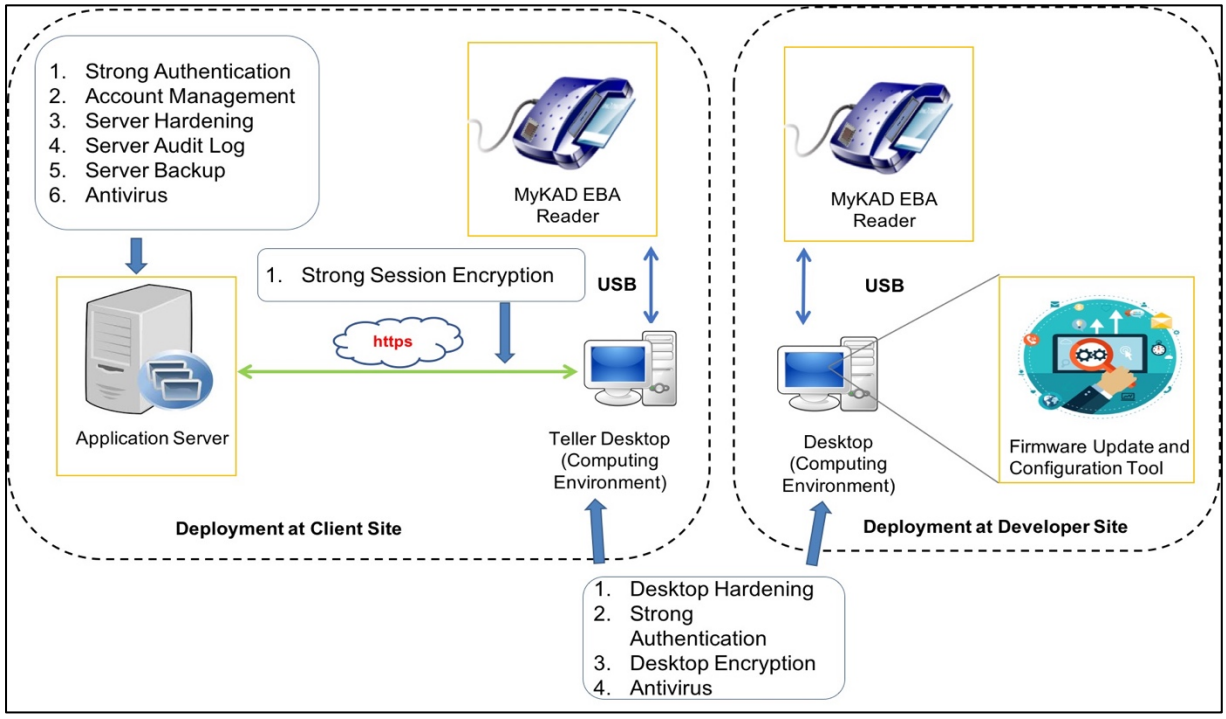

Figure 5.4 Security Control - Client-Server Computing Environment

Similar to security controls in personal computing environment, this environment also needs desktop hardening, strong authentication, desktop encryption and antivirus implemented at the Client's and Developer's desktop.

Security controls such as strong authentication, account management, antivirus, hardening, audit log and backup can be deployed at the client's site server. The session between the server or desktop at client's sites should be encrypted to avoid eavesdropping and man in the middle attack.

5.3.3 Security control - distributed computing environment

Figure 5.5 describes the security control points that should be implemented in a distributed computing environment.

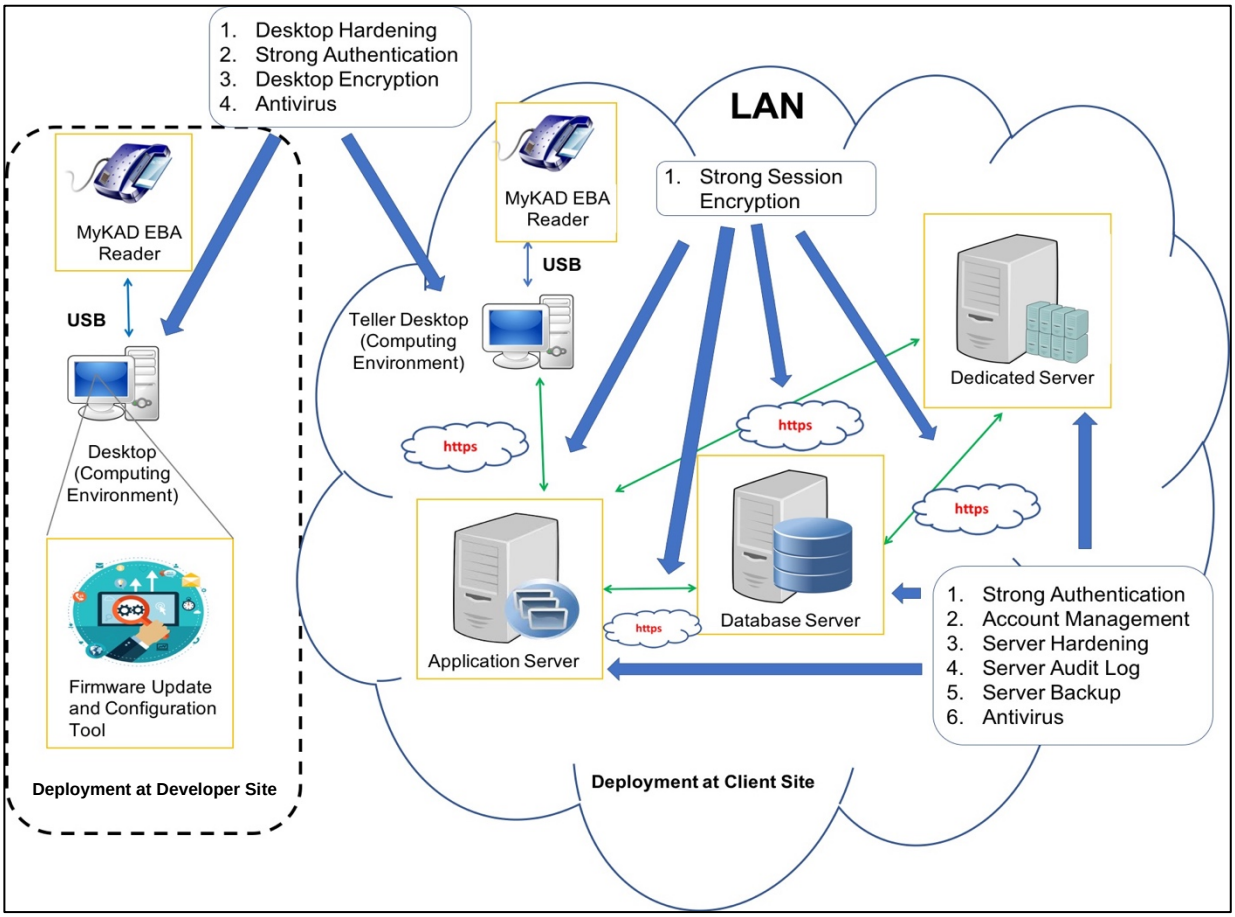

Figure 5.5 Security Control - Distributed Computing Environment

In term of distributed computing environment, dedicated, application and database servers will be in the client's Local Area Network (LAN), therefore, security controls such as strong authentication, account management, antivirus, hardening, audit log and backup should be deployed. The LAN connection should have strong session encryption between the servers and teller's desktop.

5.3.4 Best practices for security controls

This sub section briefly describes best practices for several security controls that are recommended to effectively address security needs of applications, servers and network infrastructure. Among these practices include [10][11][12]:

a) Account Management
Account management is important to protect the network from insider threats. It helps organizations to mitigate unauthorizes access through secure access management and control. Recommended practices include to implement strong authentication or multi-factor authentication (MFA), manage

privileged access, manage administrative credentials by removing users or groups that are no longer active, and to perform log analysis.

b) Application
   i) As the threats to applications increase, there is a need of a structured approach for managing the security of the applications. ISO27001 is the international standard for information security management best practice and is the most comprehensive standard for information security. It provides a framework to manage the security of applications which is also applicable for MyKAD EBA implementation. ISO27001 defines controls for the acquisition, development, customisation, maintenance and operation of applications. The controls are process-centric and technology-independent, thus making the standard strong. However, the standard does not specify the technical details for the controls. organizations should refer to detailed technical guidance available from specific application developers, from industry forums and other sources of good practices.
   ii) Application vulnerabilities can be referred Open Web Application Security Project (OWASP) and Common Weakness Enumeration (CWE). Examples of security vulnerabilities are Buffer Overflow, Failure to protect sensitive data and Broken Authentication.

c) Hardening
   Hardening is a collection of steps taken to reduce security vulnerabilities of network devices such as desktops or servers. These steps include regularly update operating system, software and applications patches, use encryption to encode sensitive information, disable file sharing, install personal firewall, remove non-essential programs, perform regular scheduled backups and implement robust password policies.

d) Networks Segmentation and Segregation
   Network segmentation separates network into segments or functional units based on their functionalities. For example, one unit dedicated for sales, and another for technical supports. This can be done through the use of routers, switches or virtual local area networks (VLANs) Segmentation provides a secure mechanism to prevent intruders from getting inside the network to access sensitive data hence help to limit the potential damage. It also helps in classifying and protecting data.

e) Validate Integrity of Hardware and Software
   Hardware and software that are acquired from unauthorized channels or dealers present a serious risk to the overall integrity of the network environment. These products that may have not been thoroughly tested or met certain quality standards can harm the network by compromising network performance and confidentiality. Hence, a periodical check on the integrity of software and hardware is important. In addition, any devices to be used in the network should be registered first with the network to avoid any integrity issues.

f) Penetration Testing
   i) It is recommended for organization to perform penetration testing annually. Penetration testing is an essential component of any ISO 27001, from initial development through to ongoing maintenance and continual improvement.
   ii) The nature of information technology assets means they may have many technical vulnerabilities that could be exploited by external attacks. These vulnerabilities include un-patched software, inadequate passwords, poorly coded websites and insecure applications.
   iii) The penetration test results will identify vulnerabilities in detail, together with the threat that can exploit them, and will usually also identify appropriate remedial action. The identified threats and vulnerabilities will then form a key input to organization's risk assessment.

5.3.5 Location

Considering every factor, the most likely target of an attack is where the transaction take place. One aspect that is prone to attack is the physical location of MyKAD EBA reader.

Organization selects and manages MyKAD EBA reader location based on various reasons and requirements. This includes but is not limited to the nature of the transaction being carried out, the card holder's needs, the cost to operate the facility and the ability to access safety and environmental issues required for the business.

Examples of locations are counters, kiosks in organization buildings and kiosks in public places. Each location has its own risks. Therefore, we need to minimize the expected risks.

a) Counter
   MyKAD EBA reader should be located at a difficult place for non-authorized personnel to access. Example, the reader is placed at the counter and the computing environment connected to the reader is located in a hard to reach place. This is to ensure the attacker cannot easily unplug the reader unless the attacker sneak into the counter. The counter should be restricted for authorized personnel only. Physical security needs to be implemented such as access door through pin number or biometric access.

b) Kiosk
   A kiosk is a small, free-standing booth or unit that is used to display information or provides services to customers. Kiosks can be categorised into manned or unmanned (self-service) kiosks and are typically placed at the organizations' premise or public area. Unmanned kiosks feature interactive self-service capabilities.
   Unlike counters, an unmanned or self-service kiosk has a much higher risks when located at public areas. This is because such locations are easily accessible to anyone. Hence, it is advisable for kiosks not to be placed too far away from main or public route. There should be good lighting to ensure that people will notice if something suspicious is happening. CCTV and alarm systems are also important. If the kiosk is placed at the organization's premise, the organization has the right to implement security system which make it easier to monitor. The organization needs to ensure that there are security personnel to monitor the kiosk, physical security systems such as CCTV and system alerts are installed in case of intrusion and the kiosk is placed in a well-lit area.

5.4 Layer 4: MyKAD EBA users security controls

5.4.1 Security awareness

IT Security Awareness is important to ensure that the organization continuously maintain a secure implementation of MyKAD EBA Ecosystem. Although MyKAD EBA reader is uniquely designed with enhanced security features, its implementation still requires a secure operational environment.

In the organization's environment, there are threats that come from different angles in which most of the threats are from human factors such as unethical behaviour, misused of IT assets and refusal to follow proper procedures. The organization's IT personnel and operators may be regarded as the main targets for committing crimes. The crimes committed may not be on their own accord but are paid by third parties. Therefore, organization need to be careful and carry out precautionary measures. Among the steps that can be taken are:

a) Do not assign the responsibilities to only one IT personnel or operator;
b) Rotate responsibilities of IT personnel or operator;
c) Monitoring by the superior; and
d) Hold awareness session to IT personnel or operator including the types of frauds that criminals can try and put the workers at risks. IT personnel or operator need to understand the mandate given and

the need to ensure that they are not involved with the crime that will harm the ecosystem and facilitate them.

Awareness program to new IT personnel or operators are crucial. Apart from the awareness not to break the trust, knowing how to protect MyKAD EBA reader and its infrastructure is equally important. They also need to be aware of what they need to consider and the actions to be taken if something happens. All IT personnel or operators need to understand:

a) Who needs to be contacted and trusted to report security breaches related to the MyKAD;
b) How to make an effective report (e.g. IT incident report) for the higher level management to have their statement to be taken seriously;
c) How to contact higher level management if they found any threat; and
d) How the management or IT personnel and operators should contact local law enforcement if someone threatens or attempts to bribe them to compromise.

In addition, card holders need to be aware when doing any transaction involving MyKAD EBA by taking several actions for example observe what tellers do with the card, know the type of transaction, make sure to receive the right card after the transaction, alert with scammers and to make sure that there is no suspicious devices placed at the kiosk.

It is imperatives for continuous awareness is required throughout the organization to ensure all relevant parties both internal and external personnel or participants of the organization uphold the policies, procedures and proper operations for future benefits in reducing risk of threats.

Bibliography

[1] European Commission, “CE marking.” [Online]. Available: http://ec.europa.eu/growth/single-market/ce-marking/.

[2] Malaysian Standard, “Multipurpose Smart Card Part 1: General Characteristic Code of Practice MS 1960,” 2007.

[3] “80pc illegals got MyKAD via fraud,” *Daily Express*, 2018. [Online]. Available: http://www.dailyexpress.com.my/news.cfm?NewsID=126801. [Accessed: 02-Oct-2018].

[4] R. Murali, “Fake MyKADs sold to foreigners,” *The Star Online*, 2017. [Online]. Available: https://www.thestar.com.my/news/nation/2017/04/28/fake-mykads-sold-to-foreigners-syndicate-charging-up-to-rm10000-for-counterfeit-ids/. [Accessed: 02-Oct-2018].

[5] Department of Standards Malaysia, “MALAYSIAN STANDARD Government Multipurpose Card - Part 2 : Data practice,” 2015.

[6] National Registration Department, “MyKAD Command Set.” [Online]. Available: http://www.jpn.gov.my/en/informasimykad/mykad-command-set/. [Accessed: 22-Nov-2018].

[7] ISO, " ISO/IEC 27001 Information Security Management - Preview." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. [Accessed: 10-Sept-2019].

[8] ISO, "ISO/IEC 27002 Information Security Management - Code of Practice for Information Security Controls." 2013.

[9] Netwrix Blog. "Top 10 Most Common Types of Cyber Attacks." [Online]. Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/. [Accessed: 14-Aug-2019].

[10] Netwrix, "Network Security Best Practices." [Online]. Available: https://www.netwrix.com/network_security_best_practices.html. [Accessed: 14-Aug-2019].

[11] CISA, "Securing Network Infrastructure Devices." [Online]. Available: https://www.us-cert.gov/ncas/tips/ST18-001. [Accessed: 14-Aug-2019].

[12] S. A. Vinod Vasudevan, Anoop Mangla, Firosh Ummer, Sachin Shetty, Sangita Pakala, *Application security in the ISO27001:2013 Environment*. IT Governance Ltd, 2015, 2015.

Acknowledgements

CyberSecurity Malaysia would like to express our appreciation and gratitude to all members of Technical Committee on Guidelines for Securing MyKAD Enhanced Biometric Access (EBA) Ecosystem who have participated tirelessly in the development of this guideline. Members are as follows:

Ts. Dr. Solahuddin Shamsuddin/	CyberSecurity Malaysia
Ts. Dr. Maslina Daud/	
Mr. Ahmad Dahari Jarno/	
Ms. Azatulsheera Mohd Azman/	
Mr. Amiroul Farhan Roslaini/	
Mr. Farhan Arif Mohammad/	
Mr. Mohd Muslim Mohd Aruwa/	
Ms. Norahana Salimin/	
Ms. Noraziah Anini Mohd Rashid/	
Ms. Noor Asyikin Zulkifli/	
Ms. Nor Zarina Zamri/	
Ms. Nur Iylia Roslan/	
Ms. Nur Sharifah Idayu Mat Roh/	
Ms. Nurul Izratul Imrah Zolkafle/	
Mr. Wan Shafiuddin Zainuddin/	
Ms. Zarina Musa	
Dr. Maryam Shahpasand	Asia Pacific University of Technology & Innovation (APU)
Mr. Jason Wong	Dermalog Biometrics Sdn Bhd
Mr. Muzaffar Tajuddin	Flow Studios Sdn Bhd
Ms. Connie Yee/	IRIS Corporation Berhad
Ms. Evelyn Laiyap Goduli	
Ms. Hafizah Abdullah/	Malayan Banking Berhad
Ms. Irma Mohd Aris/	
Ms. Raja Nor Aziah Raja Mohd Nor	
Mr. Chew Hoong Wei	MCS Microsystems Sdn Bhd
Mr. Mohammad Amirrul Rashid Zainudin/	National Cyber Security Agency (NACSA), Malaysia
Ms. Siti Hajar Roslan	
Ms. Ainon Mat Jusoh	National Registration Department (NRD)
Ms. Aumuhaimi Md. Yusof/	
Ms. Izyanie Mustafar/	
Ms. Mazni Yanti Mohd Hamer/	
Ms. Rohayu Abdul Rahim	
Ms. Zuhaidah Othman	Optima Klasik Sdn Bhd
Ms. Claudia Cho	Pradotec Corporation Sdn Bhd
Mr. Jeff Chia	RHB Bank Berhad
Ms. Lyna Maharon	Teleawan Sdn Bhd
Mr. Lim Shoo Ling	The Association of Banks in Malaysia (ABM)

Ir. Dr. Ahmad Nizar Harun — The eCeos Sdn. Bhd.
Dr. Masita @ Masila Binti Abdul Jalil — Universiti Malaysia Terengganu