Assessment of Malaysian E-Passport PKI based on ISO 27000 Series International Standards

Ahmad Iqbal Hakim bin Suhaimi, Nurulhuda Noordin, Mohd Faizul bin Ya’kub

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia

aiqbal@tmsk.uitm.edu.my, hudanoordin@tmsk.uitm.edu.my, faizulyakub@gmail.com

Abstract. Malaysia was the 1st country in the world to issue biometric passports (e-Passport) in 1998. Recent years, a number of vulnerabilities in e-Passport have been identified in the first and second generation of e-Passports. These vulnerabilities can lead to crucial security issues. Due to lack of case studies conducted to review the Malaysian e-Passport, the objectives of this study are to identify the security risk in Malaysian e-Passport PKI and to recommend the feasible solution for future enhancement. A qualitative method was used in this study where a set of interview questions prepared and interviews been conducted to four participants. The data been analyzed using Thematic Analysis and presented based on risk assessment methodology in ISO 27000 series International Standards. The risk assessment consists of two approaches; risk analysis and risk evaluation. The risk analysis identified resource identification and valuation, risk identification and risk measurement of Malaysian e-Passport PKI. While in risk evaluation, it focuses on risk mitigation and prioritizing protection activities for future enhancement. The results reveal that the Cloning, Man in the Middle, Spoofing and server related issues are the risk of Malaysian e-Passport. For recommendation, the result is to implement Password Authenticated Connection Establishment (PACE) and follow ICAO standards. The significance of this research will help policy-makers to make better decision on the future direction of Malaysian e-Passport in order to ensure Malaysian citizens having secured e-Passport.

1. Introduction

In the year of 1998, Malaysia is the first country that issued electronic passports ahead the standard published by International Civil Aviation Organization (ICAO), in which developing on the standards. The first ICAO compliant passport, known as e-Passport, was issued in Belgium in 2004 [1, 2]. E-Passport, also known as biometric passports, represent a combination between paper and electronic passport which is using biometrics to authenticate the identity of travelers [3].

Historically, passports with RFID enabled was implemented by Malaysia in 1998 is the first in the world [4]. Nevertheless, these passports were unsuccessful to maintain basic security requirements until the year of 2002, due to the passport holder information was not encrypted. Until that time, digital signature was the only security measure implemented on all the e-Passport data to ensure the integrity of the data of e-Passport.
The first of generation Malaysian e-Passports contain an image of the passport holder’s thumbprint as the biometric instead of a photograph [5]. Second generation ICAO e-Passports may also store a thumbprint template, and a small amount of writable memory for storing recent travel locations. It is noted that the RFID protocols executed by Malaysian e-Passport may also leak information.

Fingerprints are used as the primary biometric for Malaysian e-Passports [5]. There is a possibility that if unattended, spoofing these biometrics data from Malaysian e-Passport would be successful if given enough preparation time. At that time, it concluded that as Malaysian e-Passport pre-dates the ICAO standard, Malaysian passport is not compliant with ICAO and there appears to be no reliable public information on other security mechanisms.

The specifications of Malaysian e-Passport were based on the guidelines issued by the International Civil Aviation Organization (ICAO) in ICAO Document 9303 [6]. However, there were several major security threats that were improperly addressed in ICAO’s first-generation e-Passport specifications. They concluded that the first-generation e-Passport specifications have many security risks and its implementation is not advised [7].

Recent years, a number of vulnerabilities in e-Passport have been identified in the first and second generation of e-Passports. These vulnerabilities can lead to security issues such as cloning, spoofing, skimming, eavesdropping, identity theft crimes, and so on. A number of countries in European Union (EU) had taken approaches to rectify the issues and enhance the security of their e-Passports.

The switch to e-Passport requires the use of Public Key Infrastructure (PKI) to prove authenticity and integrity of those e-Passports [8]. A public key infrastructure (PKI) is a basis on which other applications, system, and network security components are built, and it is is an essential component of an overall security strategy that must work with other security mechanisms, business practices, and risk management [9].

The PKI is built to ensure that traveler’s privacy is protected. The ICAO proposes using the PKI architecture within the highest hierarchy level for each country. The ICAO PKI Technical Report is envisioned to provide standards for a simple worldwide Public Key Infrastructure, which support digital signatures applied to Machine Readable Travel Documents [10]. Each country has an independent PKI security mechanism. Each country also needs to implement and enforce proper security mechanism.

PKI is the core technology of the e-Passport verification system [11]. The e-Passport validation, achieved via the exchange of Public Key Infrastructure (PKI) certificates, is important for the interoperability benefits of e-Passports to be realized [12]. PKI validation help to prevent identity fraud and ensure the integrity of the e-Passport. Furthermore, assessment and security enhancement required before biometric recognition is considered as a viable solution to biometric security in passports.

Information security risk assessment, a major component of Information security management, aims to assist organization to identify critical treats and vulnerabilities and determine applicable countermeasures in order to manage and mitigate risk associated with the treats [13].

Several case studies on e-Passport security have been conducted. A case study on the European Union e-Passport to determine the security feature and weaknesses has resulted that both internal and external factors drive the desires for greater security in the European Union (EU) e-Passport [14]. Similar studies have been conducted on Saudi Arabia [15] and United States of America (USA) [4]. In Malaysia, similar study conducted which investigated the security issues on the Identity Card (MYKAD) [16].

On the other hand, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) has published the ISO/IEC 27000 family, a series of international standards for information security management [17～25]. The series, also known as ISO 27000 series provides globally recognised framework for best-practice information security management. Through a systematic risk management approach, the series enables a proactive method to managing security and control risk, and the ISO standards endorse strong value in security and forming a reference point for certification [26].

Therefore, the aim of this study is to conduct risk assessment of Malaysian e-Passport PKI based on ISO 27000 series international standards.
2. Methodology

This study consists of three phases. In the first phase, initial investigation on Malaysian e-Passport has been conducted with two activities. First activity is literature analysis to get the in-depth details of current Malaysian e-Passport implementation. The next activity is to construct interview questions. The outcomes of these activities are the problem statement, objective, scope, problem’s definition and interview questions.

The second phase is analysis. In this phase, a set of interview questions have been prepared, and then distributed to the selected four participants that having wide experience in Malaysian e-Passport implementation. The interview questions consist of open-ended questions and divided into 6 segments; Introduction, Resource Identification and Valuation, Risk Identification, Risk Measurement, Risk Mitigation and Recommendation.

The interviews with the four participants have been conducted with the audio recordings of the interview were transcribed in full. The next activity is to analyze the interview transcripts. The outcome from these activities is the research themes.

In the third phase, by performing Thematic Analysis activity, the risk of Malaysian e-Passport been identified and a list of recommendations have been projected. The results have been arranged based on ISO 27000 international standards.

2.1. Research Method

Interview was used as the main research instrument for this research. A set of same interview questions has been submitted to selected respondents before interview conducted. The interview question consists of open-ended questions is divided into 6 segments; Introduction, Resource Identification and Valuation, Risk Identification, Risk Measurement, Risk Mitigation and Recommendation. These questions are designed to associate with ISO 27000 frameworks for Risk Assessment.

Interview is chosen as the main method for this study due to this risk assessment of e-Passport PKI is very technical in nature and the number of expertise on this field is limited.

2.2. Participants

The participants of the interview session play important role in determining the study objective being achieved. In order to be eligible for the interview, the participant must have been experienced in Malaysian e-Passport software development life cycle (SDLC) at least 3 years. The selected person shall have the most technical knowledge on Malaysian e-Passport technologies especially on Public Key Infrastructure (PKI) and able to make good judgment and review on current system implementation. For this study, four participants have been selected as shown in Table 1.

| Participant | Designation                               | Experienced |
|-------------|-------------------------------------------|-------------|
| R1          | Senior Software Engineer (PKI Certification) | 9 years     |
| R2          | Software Engineer (Chip and Cryptography)  | 8 years     |
| R3          | Senior Software Engineer (Development)     | 7 years     |
| R4          | Project Manager (e-Passport Solutions)     | 3 years     |

Table 1. List of Participants
2.3. Interview Procedure

Before interview session been conducted, invitation letters have been sent to the selected participant to get their consent for the interview. Since the interview is technical in nature, the interview question has been prepared and shared to the participant first. The same set of interview questions are given for all participants. Based on the agreed date and time, the interview session is held in average 30 minutes. A refined question might be asked if the participant can’t understand the scope of the questions asked. All interviews were conducted in person and audio recorded and then transcribed.

2.4. Method of Data Analysis

Interview data have been transcribed and was analyzed using thematic analysis. As interviewee’s feedback are not generally immediately apparent in interview data, thematic analysis method was used to identify implicit ideas beyond explicit words or phrases and to categorize themes and issues addressed in the interviews.

2.5. Thematic Analysis Procedure

The actual analysis was conducted in accordance with well-described thematic analysis guidelines. The procedure involved as following:

i. Audio recordings of the interviews were transcribed in full and transcriptions were re-read after cross-checking to ensure accurate representation of the recordings.

ii. The words, phrases, sentences and paragraphs were deductively analyzed in accordance with research aim and coded from the transcriptions. They were given a distinctive color in the transcriptions using QDA Miner software.

iii. Coded words were again collated at a higher semantic level using QDA Miner software and were interpreted as intermediate themes beyond explicit words. Transcriptions were read again to search for other themes that were missed, and themes were identified when recurring in the data.

iv. Some of the themes were discussed for consensus and reworded where few discrepancies emerged.

v. After reviewing process, the themes were regrouped, defined and named as final themes.

2.6. Research Model

This study adopted the Information Security Risk Assessment model from ISO 27000 series. The risk assessment is combination of risk analysis and risk evaluation. Risk assessment offers a systematic technique for any organization to acquire an all-inclusive view of existing information security risks and their consequences, and the countermeasures to manage with them [26] as shown in Table 2.

Table 2 shows the risk assessment approach, segment (component) and deliverable that can be achieved from the approach. Risk analysis recognizes the valuable information assets under a system and also the vulnerabilities inside it. It also exposes threats that exploit these vulnerabilities and weaknesses which risk the organization. Finally, evaluate the possible damage and potential losses as the effect come from those risks [27]. Risk evaluation is the process of rating risk exposures on a scale with accepted risk criteria. This is performed to define the importance of each risk.
Table 2. ISO 27000 Series Risk Assessment

| Approach          | Description                                                                 | Segment                          |
|-------------------|------------------------------------------------------------------------------|----------------------------------|
| Risk Analysis     | Review of the risks associated with a particular event or action.            | Resource Identification and Valuation |
|                   |                                                                              | Risk Identification               |
|                   |                                                                              | Risk Measurement                  |
| Risk Evaluation   | Determine whether a specified level of risk is acceptable or tolerable.      | Risk Mitigation                   |
|                   |                                                                              | Prioritizing protection activities |

3. Findings and Discussion

3.1. Interview Analysis

From the audio recording, full transcription for every participant was re-read after cross checking to ensure accurate representation of the recordings. By using QDA Miner software, the words, phrases, sentences and paragraphs were analyzed and color-coded from the transcription. Coded words were again collated at a higher semantic level and interpreted as intermediate themes beyond explicit words.

All transcriptions were read again to search for other themes that were missed, and themes were identified when recurring in the data in participant’s transcription. The final themes for this research after the reviewing process, emerged from the analysis is summarized.

The number of the final theme appeared, by combining all transcription, is displayed in column Count. The number of participants which expressed the selected theme during the interview session is shown in column Cases.

The % Cases is referring to how many participants mentioned the selected theme in the interview out of total number of participants as calculated in (1).

\[
\text{% Cases} = \frac{\text{Number of participants mentioned the selected theme}}{\text{Total participant}} \times 100 \quad (1)
\]

As a comparison to all the themes found in the analysis, the % themes referring to percentage the selected themes found, in comparison of all total themes coded in the analysis as calculated in (2).

\[
\text{% Themes} = \frac{\text{Count of selected theme appearance}}{\text{Total Count of all themes}} \times 100 \quad (2)
\]

For the Risk Analysis, the Table 3 shows that there are four themes extracted from transcript. The results are cloning, main in middle attack, spoofing and server related issues. The highest appearance of themes is spoofing, whereby all four participants mentioned about it during interview session.
Table 3. Theme Frequency for Risk

| Theme                  | Description                                                                 | Count | % Themes | Cases | % Cases |
|------------------------|-----------------------------------------------------------------------------|-------|----------|-------|---------|
| Cloning                | Make an identical copy of the passport                                       | 5     | 10.0%    | 3     | 75.0%   |
| Man in the Middle      | Attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other | 4     | 8.0%     | 2     | 50.0%   |
| Spoofing               | Attacker or malicious program successfully acts on another person's behalf by impersonating data | 8     | 16.0%    | 4     | 100.0%  |
| Server Related Issues  | All servers, hardware and network related issues that may cause security breach. | 2     | 4.0%     | 1     | 25.0%   |

From the Thematic Analysis, it shows that distribution of keywords (number of cases) on four items as shown in Fig. 1. The item with the highest cases is spoofing while the least is server related issues. Therefore, there are four risks have been identified. There are cloning, man in the middle, spoofing and server related issues. For Risk Evaluation, a number of themes for recommendation emerged and summarized as per Table 3.

The result in Table 4 shows two very significance themes appeared in the interview transcription. All participants did mention on Follow ICAO Standards as the main recommendation, and most participants (3 out of 4) suggested on Implement PACE as their solutions to the risk issues.

Therefore, there are two recommendations have been identified from the Thematic Analysis. There are to implement Password Authenticated Connection Establishment (PACE) and to follow International Civil Aviation Organization (ICAO) standards.
**Table 4. Theme Frequency for Recommendation**

| Theme               | Description                                                                 | Count | % Themes | Cases | % Cases |
|---------------------|-----------------------------------------------------------------------------|-------|----------|-------|---------|
| Implement PACE      | Password Authenticated Connection Establishment (PACE) protocol, which specified by Supplementary Access Control (SAC) | 11    | 22.0%    | 3     | 75.0%   |
| Follow ICAO Standards| The International Civil Aviation Organization (ICAO) standards for e-Passport | 11    | 22.0%    | 4     | 100.0%  |

**Fig 1.** Number of Cases Mentioned according to Risks
3.2. Cloning

A group of interrelated themes have highlighted about passport cloning. When asking on the risk that can be occurred in Malaysian e-Passport, a participant which is a senior engineer, is very confident on the risk chosen.

“As mentioned, passport cloning”. (R3)

This statement is supported by another participant, a senior engineer, that detailing the passport cloning. He elaborated on how the passport cloning can be created by exploiting the chip architecture and the data. This may be assisted by chip manufacturers, vendors or any expertise that having wide knowledge on chip’s material and design.

“If the passport or the chip vendor or chip architecture or chip information is leaking, or the hacker able to reconstruct the chip because they got the way to create the chip, or they get information how to generate the new passport, and they got the material – it will causing the problem when they are able to regenerate or personalization the passport with any name or holder information”. (R1)

Besides cloning the data, there is also possibility risk of cloning the secure PKI certificate. A participant in the interview had mentioned that the cloning of the PKI security key in Malaysian e-Passport is possible. One of the examples is when there is a supercomputer that able to do high processing with faster speed. Once the keys that protect the data broken and the attacker would be able to decrypt the data inside the passport chips and perform the cloning.

“Let say we have supercomputer, (the hacker) will generate the key pair from the paddle” (R2)

3.3. Man in the Middle

Man in the Middle attack can occur when attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other from the paddle.

The possible source of the attack mentioned by the participant during the interview is due to the implementation of Extended Access Control (EAC) mechanism which currently does not complying with the standards. This means that the implementation is partially completed due to the usage is not as per what is supposed to be. Thus, give a room for opportunity for the attacker to exploit the system incompleteness to launch the Man in the Middle attack or altering the communication in between. Take note that the e-Passport is equipped with RFID, thus stealing those data in between in unsecure communication is very much possible.

“Malaysia passport currently we only got implement until EAC part, but we didn't use properly for this EAC as per other countries” (R2)

For the protection of personal biometric data, EAC-enabled e-Passports impose a much strong mutual authentication between the chip and the reader. This is done before biometric data is released. If not implemented, this may cause Man in the Middle attack. A participant, during the interview, stated the reason why he mentioned that for Malaysian e-Passport due to the implementation is partial completed.

“In term of completeness, it is partially complete. Like the TA, they use only in Malaysia only. And overseas (foreign passport) didn’t use.” (R2)

Based on his explanation, he means that the EAC-enabled passport currently only checks Malaysian passport, but it does not check for foreign passport at the Malaysia border control system using EAC system.
In another interview session, a participant also highlighted a similar finding. He mentioned what will happen if PKI mechanism is not implemented properly or incomplete. He mentioned that the attacker might steal the data during authentication process. The authentication process is part of the passport verification to ensure the passport integrity.

"The risks if the PKI mechanism not implemented properly. So, let say we have the Extended Access Control (EAC) Mechanism, but somehow our system not complete or got the security issue, it maybe will let the hacker to steal the information during the authentication process. Or let say BAC (Basic Access Control) or Passive Authentication process not fully completed, or the key maybe leaking, or the data not fully encrypted, it will end up the hacker or the certain party can steal the data, or if eavesdropping the information during authentication process.” (R1)

This eavesdropping of information during authentication process is related to Man in the Middle attack in e-Passport. By eavesdrop the communication line; the secure data can be extracted. He also further described that the risk in Malaysian e-Passport due to the passport does not comply with the International Civil Aviation Organization (ICAO) standards.

"If the systems they setup not comply to certain standard like ICAO standard, it will have higher risk to be attacked by the hacker, either by network or insider can access the system to steal the information.” (R1)

3.4. Spoofing
This theme is related to attacker or malicious program successfully acts on another person's behalf by impersonating data. This is another security in Malaysian e-Passport and highly mentioned during the interview. The main reason of this spoofing can occur is due to Malaysia does not implement Biometric face and iris.

This statement is agreed by most of the participant which noted that the verification of iris, a method of identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye, is not exist in current Malaysian e-Passport solution.

"Currently, we no verify the iris” (R1)

The statement also supported by another participant. However, the lacking on Iris verification is not the only missing part in the e-Passport. Malaysian e-Passport is also lacking on Biometric face verification in its current implementation.

"The biometric face I think not yet, and the iris also not yet.” (R2)

If biometric verification does not implement fully, there is a risk and possibility of impersonation and spoofing to occur. A participant even explained the reason of this issue due to the information leaking. Thus, when a passport has been cloned, an impersonation risk is high.

"If the passport or the chip vendor or chip architecture or chip information is leaking or the hacker able to reconstruct the chip because they got the way to create the chip” (R1)

Most participants summarized this case with a strong statement that the e-Passport used by current Malaysian does not having the latest security mechanism. Thus, the risk mentioned is real and hard to be avoided.
3.5. Server Related Issues

Besides the risk on cloning, man in middle attack and spoofing issues, there is another type security risk in Malaysian e-Passport system. This risk is related the hosting of the system servers. The participant would like to emphasise that the server might be down or not in operation for certain time due to hiccup. She even mentioned the possibility this risk to occur is high.

“The likelihood for the server down is high” (R3).

The server down risk issue shall be taken seriously, due to any flaw to the server might give the needed time by attacker to exploit the security weaknesses. For example, when the server is offline temporarily, the critical services such as Inspection System at the border control could be affected in such way that online passport verification, checking to blacklisted database, passport authentication and biometric verification would be halted.

3.6. Risk Measurement

When asking on the likelihood and the impact of those risks to be occurred, the participants have stated different their opinion on the matters.

A project manager is opinioned that the likelihood of the mentioned risk and its impact if that happen is high. Based on experience, he has a wide experience in project management, and currently overlooks a group of e-Passport project managers in his departments.

“High.” (R4)

However, a software engineer has different view on the possibility of risk likelihood. He has opinion that the likelihood of these risk mentioned to occur is low since so far none of the risk is ever breached yet. On the other hand, he was opinioned that the impact is still high if that risk really occurred.

“The likelihood is low to happen.” (R2)

“For the passport itself, it is secure already. I will give (rating) 3 to 3.5 (out of 5) for impact” (R2)

Similar to his view, another participant, a Senior Software Engineer, has view that the likelihood might be low to medium. However, he still opted that the impact is still high.

“If the 1 is lowest (and 5 is the highest), I can see the number is around maybe 2 or 3. I think maybe 2 for the current stage” (R1)

In summary, most participants mentioned that the likelihood of occurrence of the risk found in Malaysian e-Passport could be low, but the impact of the risk is high. This indicates how seriousness the effect of the threats in securing the personal biometric data inside the traveler’s e-Passport.

3.7. Risk Mitigation

All participants have same unanimous view on risk mitigation – to avoid the risk at all cost. This is due to the impact of the risk is high, and all preventive measure should be implemented from beginning until the end.

The way they answered the question indicated that the risk is not tolerable especially when involving stolen of biometric data such as fingerprint to the attacker. Missing a biometric is not equal to missing a password. Password can be replaced, but biometric data is permanent and cannot be replaced. The data kept by the attacker forever.
“We should avoid it. We don’t want the risk occur at all, or minimize it” (R2)

“I think – what can I say is – we are under to avoid the security risk. Avoid at initial stage” (R1)

“Avoid. Considering the above mentioned solution instead” (R4)

“ICAO already defines probably for the risk. We should avoid” (R3)

This evidence is clearly shown that all participants have the same view on the risk mitigation which is to avoid the risk from occurring at all. This is understandable, as based on the risk measurement, the risk impact is high. Thus, as the high-risk impact to the travellers, it should be avoided at all.

3.8. Recommendation

3.8.1. Implement Password Authenticated Connection Establishment (PACE)

Supplemental Access Control (SAC) is a set of latest security features defined by ICAO for shielding data contained in electronic travel documents e-Passport. SAC stipulates the Password Authenticated Connection Establishment (PACE) protocol, which complements and enhances ICAO’s Basic Access Control (BAC).

The participants have the view that this new third generation e-Passport solution, which applying the latest security technology, shall be implemented in Malaysian e-Passport PKI. third generation of e-Passport is the replacement of Basic Access Control (BAC) with Supplementary Access Control (SAC) [26]. In the SAC- PACE solutions, the weaknesses of the first and second generation e-Passport have been solved.

“Soon, in my opinion, Malaysia will also going to implement this SAC PKI method to ensure the passport is having the latest security technology to prevent all possible risks in the future” (R4)

He added that the solution is the better options due to the secure data communication between the chip and the reading devices, and also the protection of the contactless chip from being read without physical access to the travel document.

“SAC is an evolution of BAC aimed at ensuring future-proof security in electronic travel documents. It is similar in function to BAC and ensures that the contactless chip cannot be read without physical access to the travel document and that the data exchange between the chip and the reading device is encrypted” (R4)

This view is shared by another participant. His opinion is the SAC-PACE technology will speed up the reading and authenticating a Malaysian e-Passport, and this solution is more secure and enhancing the previous Chip Authentication (CA).

“You want to cut through all the process, you have to replace by PACE (Passport Authenticated Connection Establishment). The CA replaced by PACE will become more faster.” (R2)

He further compared the PACE better than EAC and mentioned that more countries migrate from EAC to PACE protocol.

“We can implement the SAC (Supplementary Access Control) or the passport can upgrade to EAC. Because the PACE become more like EU region, and implemented by EU in certain countries, not all. Most important is EAC. But now they migrate to PACE. PACE is SAC.” (R2)
Another participant has similar view. She stated that, PACE is suggested by an ICAO. Even though the implementation is not mandatory for all countries, the solution can enhance the security level of e-Passport greatly.

“Add PACE security mechanism as suggest by ICAO to increase the security level” (R3)

In summary, majority of the participant suggested PACE as a solution for the risk in Malaysian e-Passport. PACE mechanism is categorized under third generation of e-Passport and introduced as a replacement to the Basic Access Control (BAC) mechanism [3]. PACE ensures the verifier has physical control over the e-Passport, and prevent remote access and remote tracking to data stored on the e-Passport [28].

3.8.2. Follow ICAO Standards

In addition, participants also suggest that Malaysian Authority to look into improvement of current standard. They have opinioned that one of the main reasons of the risks in Malaysian e-Passport is due to incompleteness of the e-Passport security - incomplete to implement the latest standard, and incomplete to implement the e-Passport solution according to the chosen standards.

Participant also agreed that the PKI mechanism published by International Civil Aviation Organization (ICAO) is a comprehensive mechanism and authority shall review the current implementation to ensure it is adhered to the latest standards.

“Follow ICAO procedure to implement all those security mechanisms. ICAO procedures already manage the risk.” (R3)

“Follow the latest security mechanism and the standard which recommended by the ICAO” (R1)

ICAO owns a technical document and standards named as Doc 9303 [29]. This international organization is responsible for research into travel document technologies, analysis, and the development of strategies, policies, and new as well as amended specifications. It also contributes guidance material to explain and encourage the standardization and interoperability of travel documents.

From time to time a ‘Supplement to Doc 9303’ is issued, containing information to clarify, amplify or elaborate on issues relating to travel document standards. These Supplements also contain corrections as a result of implementation issues (and experiences).

4. Discussion

Due to BAC’s weak security properties, the PKI protocol in Malaysian e-Passport shall be replaced by a more secure Password Authenticated Connection Establishment (PACE). PACE was developed initially as a component of the Extended Access Control version 2 [30]. The passports will apply version 2 in PACE protocol. Password Authenticated Connection Establishment (PACE) protocol is specified by Supplementary Access Control (SAC) mechanism.

PACE replaces the BAC protocol. It is a mechanism, which allows a Tag to authenticate that the Reader has authorized access to the e-Passport. Furthermore, Tag and the Reader share a shared password which is applied with the Diffie-Hellman key agreement protocol to provide a strong session key [4].

Two types of passwords are allowed with electronic passports are Card Access Number (CAN) and Machine readable zone (MRZ) passwords. CAN could be a short static or dynamic. In case the CAN is static, it can be easily printed on the passport book. On the other hand, if CAN is dynamic password, the Tag will randomly pick it and shows it on the passport by applying low power display technologies.
The technologies existed such as OLED or ePaper. Meanwhile, the MRZ password is a static type symmetric key which derived from the MRZ of the electronic passport [4].

PACE is required for privacy reasons to protect electronic data against unauthorized access, establishes a secure connection between chip and terminal and protects against skimming and eavesdropping. It was invented to overcome weakness of BAC and was designed based on asymmetric cryptography (Diffie-Hellman).

The implementation of SAC-PACE will take few years before the support of BAC can be detached from newly issued passports. This is due to compatibility reasons. Thus, if Malaysia plan to implement SAC-PACE, feasibility study shall be conducted as earliest as possible, and study on the potential and positive impact on its implementation; financial effect, public security confidence when security is protected and readiness to protect citizen from any harmful risk and security breach.

Lastly, if Malaysia implements PACE mechanisms, the implementation shall include all the ICAO standards fully and not partially. This may include all the recommendation and best practices for third generation of e-Passport. Then, Malaysian e-Passport PKI security would be greatly enhanced. This would be a major achievement to the Malaysian e-Passport solutions.

5. Conclusion

e-Passport is a very secure document, thus keep away passport forgery, reproduction and tampering. The e-Passport protect against issuing multiple passport with different identity to a same person. It also enhances in term of imposter or fraud detection. An e-Passport provides traveler benefits such as use of automated border clearance in airport, automated issuance of boarding passes, and faster travel arrangements with enforcement agencies and airlines.

The aim of this study is to conduct risk assessment of Malaysian e-Passport PKI based on ISO 27000 series international standards. From the results, there are four risks have been identified. There are cloning, man in the middle, spoofing and server related issues. This study recommends the implementation of Password Authenticated Connection Establishment (PACE) and adheres to ICAO Standards to address the identified risks.

The use of e-passport provides better border protection and security to the citizen. The issuance of e-Passports will allow Malaysia to provide world-class consular services to its nationals. Other countries shall have greater confidence and acceptance of the Malaysian e-Passport with enhanced security technology and with frequent risk assessment and risk management properly in place.

Acknowledgment
We would like to thank Faculty Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam for supporting and funding this study.

References
[1] Avoine G, Beaujeant A, Hernandez-Castro J, Demay L, and Teuwen P 2016 A Survey of Security and Privacy Issues in e-Passport Protocols ACM Computing Surveys vol 48 no 3 pp 1-37
[2] Avoine G, Kalach K, Quisquater K 2008 epassport: Securing international contacts with contactless chips Proc. Int. Conf. on Financial Cryptography and Data Security pp 141-155
[3] Atanasiu A and Mihaiescu M I 2010 Biometric passports (ePassports) Proc. Int. Conf. on Communication pp 443-446
[4] Nithyanand R 2009 A Survey on the evolution of cryptographic protocols in ePassports Cryptology Eprint Archive p 200
[5] Juels A, Molnar D, Wagner D 2005 Security and Privacy Issues in e-Passport Proc. Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks pp 74-88
[6] Saoudi S, Yousfi S, and Robbana R 2016 Protocol on the Spi Calculus Proc. Int. Conf. on
Verification and Evaluation of Computer and Communication Systems pp 161-176

[7] Sinha A 2011 A survey of system security in contactless electronic passports J. Computer Security vol 19 no 1 pp 203-226

[8] Bogari E A, Zavarsky P, Lindskog D, and Ruhl R 2012 An investigative analysis of the security weaknesses in the evolution of RFID enabled passport Int. J. of Internet Technology and Secured Transactions vol 4 no 4 pp 290-311

[9] Weise J 2001 Public key infrastructure overview Sun BluePrints OnLine pp 1-27

[10] Lekkas D and Gritzalis D 2007 e-Passports as a means towards the first worldwide Public Key Infrastructure European Proc. Int. Conf. on PKI workshop pp 34-48

[11] Abuadhmah NA, Naser M, and Samsudin A 2010 E-Visas Verification Schemes Based on Public-Key Infrastructure and Identity Based Encryption J. Computer Science vol 6 no 7 p 723

[12] Srinivasan B 2013 Security and Privacy in E-Passport scheme using Authentication Protocols and Multiple Biometrics Technology Int J. Computer Science and Business Informatics vol 3 no 1 pp 1-16

[13] Khidzir NZ, Mohamed A, and Arshad NH 2010 Information security risk factors: Critical threats vulnerabilities in ICT outsourcing Proc. Int. Conf. on Information Retrieval & Knowledge Management pp 194-199

[14] Ng-Kruelle G, Swatman P A, Hampe J F, Rebane D S 2006 Biometrics and e-Identity (e-Passport) in the European Union: End-user perspectives on the adoption of a controversial innovation J. Theoretical and Applied Electronic Commerce Research vol 1 no 2 pp 12-35

[15] Khan B, Khan M K, and Alghathbar K S 2010 Biometrics and identity management for homeland security applications in Saudi Arabia African J. of Business Management vol 4 no 15 pp 3296

[16] Kee Y A, see Y C, Beng L Y, and Fun T S 2012 Security Issues on Identity Card in Malaysia Int. J. of Engineering and Technology vol 4 pp 617 – 621

[17] Disterer G 2013 ISO/IEC 27000, 27001 and 27002 for information security Management J.of Information Security vol 4 no 2 pp 92 – 100

[18] ISO/IEC 27000 2018 Information security management systems - Overview and vocabulary ISO

[19] ISO/IEC 27001 2013 Information technology - Security techniques - Information security management systems – Requirements ISO

[20] ISO/IEC 27002 2013 Information technology - Security techniques - Code of practice for information security controls ISO

[21] ISO/IEC 27003 2017 Information technology - Security techniques - Information security management systems – Guidance ISO

[22] ISO/IEC 27004 2016 Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation ISO

[23] ISO/IEC 27005 2018 Information technology - Security techniques - Information security risk management ISO

[24] ISO/IEC 27006 2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, ISO

[25] ISO/IEC 27007 2017 Information technology - Security techniques -- Guidelines for information security management systems auditing, ISO

[26] Barlette Y and Fomin V V 2008 Exploring the suitability of IS security management standards for SMEs Proc. Int. Conf. on System Sciences p 308

[27] Shameli-Sendi A, Aghababaei-Barzegar R, and Cheriet M 2016 Taxonomy of information security risk assessment (ISRA) J. Computers & Security vol 57 pp 14-30

[28] Hermans J, Peeters R, and Bunchmann N 2017 epassport Protocols And Certificate Architecture J. IET Biometrics vol 7 no 4 pp 356-364

[29] Heitmeyer R 2010 ICAO Civil Aviation and MRTD Standards J. of Documents & Identity vol 31 pp 1-6

[30] Riha Z and Matyas V 2011 Privacy Issues of Electronic Passports J. of Medical Informatics & Technologies vol 17 pp 37-48