An On-Line Secure E-Passport Protocol

Vijayakrishnan Pasupathinathan[1], Josef Pieprzyk[1], and Huaxiong Wang[2]

[1] Centre for Advanced Computing - Algorithms and Cryptography (ACAC)
Department of Computing
Macquarie University, Australia
{krishnan,josef}@ics.mq.edu.au
[2] Nanyang Technological University, Singapore
hxwang@ntu.edu.sg

Abstract. The first generation e-passport standard is proven to be insecure and prone to various attacks. To strengthen, the European Union (EU) has proposed an Extended Access Control (EAC) mechanism for e-passports that intends to provide better security in protecting biometric information of the e-passport bearer. But, our analysis shows, the EU proposal fails to address many security and privacy issues that are paramount in implementing a strong security mechanism.

In this paper we propose an on-line authentication mechanism for electronic passports that addresses the weakness in existing implementations, of both The International Civil Aviation Organisation (ICAO) and EU. Our proposal utilises ICAO PKI implementation, thus requiring very little modifications to the existing infrastructure which is already well established.

1 Introduction

Due to increased risk of terrorism, countries are adopting biometric enabled passport as a preventive measure to monitor and strengthen their border security. The ICAO, an United Nation body responsible for setting international passport standards, established five task forces under the New Technology Working Group (NTWG) to develop a standard for Machine Readable Travel Documents (MRTD) [1]. The ICAO standard DOC 9303 [1] for MRTD describes a contactless smart card microchip that conforms with ISO-14443 [2], embedded within an e-passport booklet. The microchip duplicates the information that appears on an passport's bio-data page and which is recorded in the Machine Readable Zone (MRZ). The e-passport standard provides details about establishing a secure communication between an e-passport and an Inspection System (IS), authentication of an e-passport, details on storage mechanism and biometric identifiers that should be used.

Ari Juels, *et al.* [3] presented some security and privacy issues that apply to the first generation e-passports. The authors express concerns regarding the fact that the contactless chip embedded in an e-passport allows the e-passport contents to be read without direct contact with an Inspection System (IS) and, importantly, with the e-passport booklet closed. The authors also raise concerns as to whether

L. Chen, Y. Mu, and W. Susilo (Eds.): ISPEC 2008, LNCS 4991, pp. 14–28, 2008.

data on the chip could therefore be covertly collected by means of “skimming” or “eavesdropping”. Because of low entropy, the key would be also vulnerable to brute force attacks as demonstrated by [4]. The risk of eavesdropping is increased by the surveillance environment in which border checks occur, particularly, as the border control becomes more and more automated (as discussed in [5]), this will ultimately assist in a covert collection of e-passport data. Kc and Karger [6] presented the “splicing attack”, “fake finger attack” and other attacks that can be carried out when an e-passport bearer presents the passport to hotel clerks.

In [7], V. Pasupathinathan *et al.* made a formal analysis and found that the e-passport protocol does not satisfy security goals for data origin authentication as it can be subject to replay and grandmaster chess attacks, and the weakness can be exploited in cases where problems with facial biometric exists. They also pointed out that data confidentiality is also compromised when an attacker is able to obtain encryption and MAC keys stored in the e-passport chip using information stored in MRZ. They were able to formally verify and prove that security goals like, mutual authentication, key freshness and key integrity are also not satisfied.

To address these concerns the NTWG has planned further discussions in 2007 about standardising the next generation of e-passports that will support Extended Access Control (EAC), which is based on EU’s proposal [8] for EAC. A primary goal of EAC is to provide mutual authentication (in particular, authentication of IS) and additional security for biometrics. The first generation e-passports have a single biometric identifier, based on the facial biometric, whereas the second generation will include both finger prints and iris scan biometric identifiers.

This paper analyses the security features of the current proposal for EAC, identifies its weaknesses and proposes an alternative mechanism. We believe that, EAC proposal fails to provide adequate security and has introduced security weaknesses and implementation issues on its own. Our proposed solution addresses the drawbacks in the current EU EAC proposal and provides the following enhanced security features: (1) prevention of biometric information being released to a malicious IS in possession of MRZ details, (2) enhancement of communication security between an e-passport and a IS, (3) protection against passport skimming and (4) reduction of PKI implementation.

1.1 Organisation

In Section 2 we provide a brief overview of EAC protocol and highlight some security issues and weaknesses in proposed authentication mechanisms. In Section 3, we propose our protocol for EAC that covers the entire e-passport protocol suite. In Section 4, we provide a security analysis of our proposed system and finally, Section 5 concludes our work.

2 EU Extended Access Control

EU has issued an e-passport specification [8] for EAC and is intended to restrict access to secondary biometric identifiers like finger prints and iris scans.

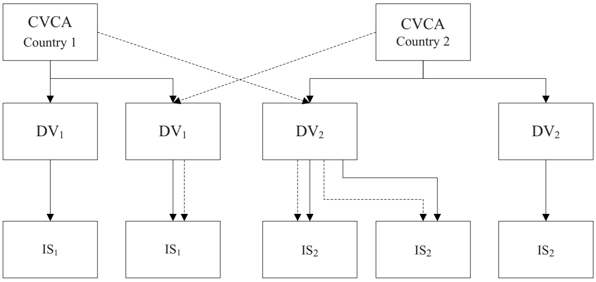

Fig. 1. EAC PKI

The guideline is based on authentication techniques proposed by D. Klüger from Federal Office for Information Security (BSI) [9,10]. Klüger proposed two protocols, Chip Authentication (CA) and Terminal Authentication (TA). His proposal also included modifications to the existing PKI. Country Signing Certification Authority (CSCA) is required to certify Document Verifiers (DV) in other countries which in turn certifies Inspection Systems (IS) present at a country's border security checkpoint. Figure 1 provides an overview of the modified PKI hierarchy.

2.1 E-Passport Operation with EAC

The EU EAC proposal for e-passports involves the following four protocols:

1. An e-passport bearer presents his/her document to a border security officer who scans the MRZ on the e-passport through a MRZ reader and then places the e-passport near an IS to fetch data from the chip. The e-passport and the IS establish an encrypted communication channel by executing the Basic Access Control (BAC) protocol (described in Appendix A).
2. The IS and the e-passport then perform a mandatory chip authentication.
3. The chip authentication is followed by passive authentication as in the first generation passport (described in Appendix A).
4. Terminal authentication.

Only if all protocols are completed successfully, the e-passport releases sensitive information like secondary biometric identifiers. If an IS does not support EU EAC, the e-passport performs the collection of protocols as specified in the first generation e-passports.

2.2 Chip Authentication (CA)

Chip Authentication protocol is a mandatory EU EAC mechanism that replaces active authentication proposed in the first generation e-passports. It involves a Diffie-Hellman key agreement and is followed by *passive authentication*. It is performed after a successful BAC and provides both an authentication of the chip and generation of a session key. The chip sends its public key ($\mathtt{PK}_{chip}$) and its

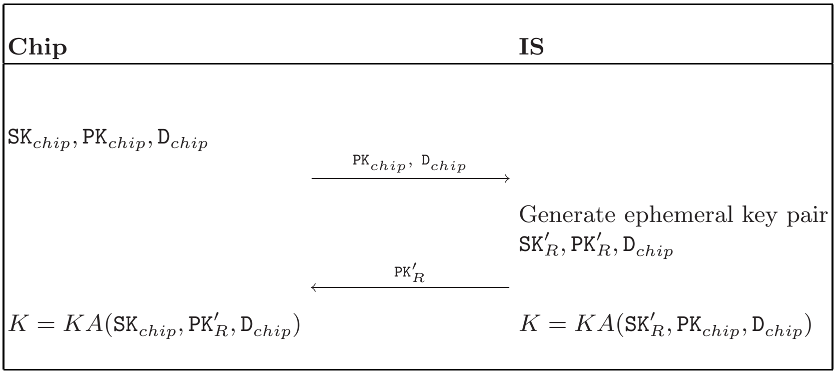
Chip
IS
$\mathtt{SK}_{chip}, \mathtt{PK}_{chip}, \mathtt{D}_{chip}$
$\mathtt{PK}_{chip}$, $\mathtt{D}_{chip}$
Generate ephemeral key pair
$\mathtt{SK}'_R, \mathtt{PK}'_R, \mathtt{D}_{chip}$
$\mathtt{PK}'_R$
$K = KA(\mathtt{SK}_{chip}, \mathtt{PK}'_R, \mathtt{D}_{chip})$
$K = KA(\mathtt{SK}'_R, \mathtt{PK}_{chip}, \mathtt{D}_{chip})$

Fig. 2. Chip Authentication

domain parameters ($\mathtt{D}_{chip}$) to IS. IS then generates an ephemeral D-H key pair ($\mathtt{SK}'_R$,$\mathtt{PK}'_R$) using the same domain parameters and sends the newly generated public key to the chip. Both the chip and IS derive a new session key K. The chip authentication is immediately followed by a passive authentication. This allows IS to verify whether $\mathtt{PK}_{chip}$ is genuine.

2.3 Terminal Authentication (TA)

Terminal Authentication is also a mandatory EU EAC mechanism that involves a two-pass challenge-response protocol and allows the chip to authenticate an IS. TA is only carried out after a successful run of chip authentication and passive authentication as it provides only an unilateral authentication of IS. During TA, the IS is required to send a certificate chain ($\mathtt{CERT}_{IS}\langle\rangle$, $\mathtt{CERT}_{DV}\langle\rangle$, $\mathtt{CERT}_{CVCA^H}\langle\rangle$). The certificate $\mathtt{CERT}_{CVCA^H}\langle\rangle$ represents a certificate issued by the e-passport's home country's CA, which is also stored in the e-passport. The

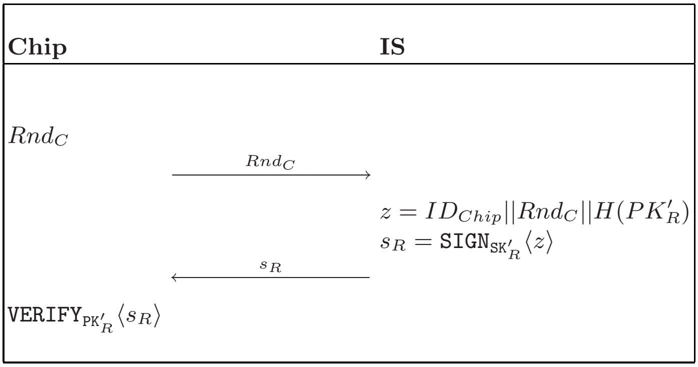
Chip
IS
Rnd_C
Rnd_C
$z = ID_{Chip}||Rnd_C||H(PK'_R)$
$s_R = \mathtt{SIGN}_{\mathtt{SK}'_R}\langle z\rangle$
s_R
$\mathtt{VERIFY}_{\mathtt{PK}'_R}\langle s_R\rangle$

Fig. 3. Terminal Authentication

chain indicates that the visiting country's IS is certified by a visiting country's Document Verifier (DV), which in turn is certified by a e-passport's home country CVCA. After a certificate chain is validated by the e-passport, it sends a challenge to IS. IS responds with a digitally signed message that contains the received challenge, the IS's ephemeral public key used in the chip authentication and e-passport ID (ID_{chip}), where, ID_{chip} is the document ID obtained from the e-passport's MRZ. The e-passport verifies the signature received and if the verification holds then it has successfully authenticated IS.

2.4 Security Issues in Second Generation E-Passports

EU proposal for EAC in e-passports provides much better security compared to the first generation e-passports. Nevertheless, EAC proposal still relies on BAC to derive the initial session key needed to access e-passport bearer's details including their facial biometric. Because of the inherent weaknesses of BAC as previously described (e.g. keys that have insufficient entropy), the EAC proposal also suffers from the same weaknesses.

EAC proposal makes extensive use of PKI. Both chip and terminal authentication protocols requires verification of certificates that invovles the entire certification hierarchy. The e-passport initially contains the root level certificate ($\mathtt{CERT}_{CVCA^H}\langle\rangle$) that was written by its document verifier at the time of issue. As the e-passport chips are time-less devices, i.e they do not have any internal clock, this makes them vulnerable to attacks using expired certificates. Klüger [9,10] acknowledges this vulnerability and proposed that the e-passport should write $\mathtt{CERT}_{CVCA^H}\langle\rangle$ with the latest certificate it obtains when it performs a terminal authentication with a visiting country's IS. During the first run of terminal authentication the time of expiry of $\mathtt{CERT}_{CVCA^H}\langle\rangle$ that was initially written is used as a reference time to validate visiting country's IS certificate and after a successful run of the protocol the e-passport will store the $\mathtt{CERT}_{CVCA^H}\langle\rangle$ that is present in the certificate chain received from an IS. But, the protocol is still vulnerable to attacks using expired IS certificates. Validity of IS certificates are considerably shorter when compared to CVCA certificates. A compromised IS even if its certificate was expired would still be able to authenticate itself to an e-passport and obtain access to sensitive e-passport information including finger prints and iris scans, that were intended to be protected by EAC. The attack is more effective for infrequently used e-passports, because they have only the initially written $\mathtt{CERT}_{CVCA^H}\langle\rangle$ which themselves may be expired. As the e-passport uses the time on $\mathtt{CERT}_{CVCA^H}\langle\rangle$ as a reference point, it would accept any certificate, as long as its validity is before the current reference time recorded on the e-passport.

The approach of sending certificate chains can also lead to a Denial-of-Service (DOS) attack on an e-passport. Since an IS terminal is not authenticated during or before chip authentication, a malicious terminal could flood the chip by sending lots of public keys and certificates. Because of the limited memory that is available in an e-passport chip, the chip could run out of memory and essentially stopping the chip from functioning in a desired manner.

The EAC proposal also has some new weaknesses. The e-passport should now have write access to the chip, to update its $\mathtt{CERT}_{CVCA^H}\langle\rangle$. This could be used by an illegitimate e-passport bearer to update the chip with false information. The EAC proposal does not specify how write access would be controlled by the chip. Another drawback of EAC proposal is the cross certification among countries. Every country implementing EAC would be required to certificate other country's document verifiers. That essentially means that each document verifier that certifies IS will need to be certified by CSVA of every participating country. EAC recommends the validity of document verifier certificates be one third of CVCA certificate's validity period. This becomes an extremely complex undertaking for each country, with respect to certifying other participating country's document verifiers and maintenance of revocation lists. EAC also does not address Grandmaster Chess Attack [11] to which the first generation passports were vulnerable to. The BAC protocol is used only to form a session key for an encrypted communication channel between a chip and IS and does not provide authentication. Therefore the chip establishes a session key even though it is not sure if IS is genuine. EU EAC also does not provide any guarantees regarding freshness or origin of messages.

There are also concerns regarding privacy of the e-passport bearer. The chip sends its identification details (public key) during CA, even before it has authenticated the IS. Therefore, this would make very easy for an attacker to track an e-passport bearer, as an attacker is not required to authenticate to an e-passport before obtaining details from an e-passport. H. Scherzer *et al.* from IBM developed a secure operating system called Caernarvon [12] for smart cards. In the Caernarvon protocol a smart card reader authenticates itself to a smart card chip using its public key first and then engages in the Diffie-Hellman key agreement to form a session key. This makes the Caernarvon protocol more secure compared to the current implementation in EAC, but the Caernarvon protocol shares the same weaknesses EAC has with certificate verification as discussed above.

3 On-Line Secure E-Passport Protocol (OSEP Protocol)

In this section we present an on-line secure e-passport protocol. An on-line authentication system for e-passport is similar to the current e-passport system (or as in the standard non-electronic passport). Currently, most security organisations are involved in passive monitoring of border security checkpoints. When a passport bearer is validated at a border security checkpoint, the bearers details are collected and entered into a database. The security organisation compares this databases against the databases of known offenders (e.g. terrorists and wanted criminals). The OSEP protocol changes this to an active monitoring system. The border security check-point or the DV can now cross check against the database of known offenders, simplifying the process of identification of criminals.

Our proposal provides the following security features:

- An e-passport discloses its information stored on the chip only after a successful authentication of IS. This prevents revealing e-passports identity to a third party that is not authorised or cannot be authenticated. This prevents covert collection of e-passport data from ”skimming” or ”eavesdropping” attacks that were very effective against both the ICAO e-passport and the EU EAC standards.

- The OSEP protocol provides proof of freshness and authenticity for messages between participating entities.
- The OSEP protocol uses existing ICAO PKI implementation (first generation passports) and eliminates the need for cross certification among participating countries as required by EU EAC (second generation passports).
- The OSEP protocol eliminates the need for certificate chain verification by an e-passport. Only the top level certificate (CVCA) is required to be stored in an e-passport chip, reducing memory requirements and thus prevents a malicious reader from performing a DOS attack on an e-passport.
- The OSEP protocol also requires an IS to provide proof of correctness for public key parameters to an e-passport. This allows an e-passport to verify that an IS is using correct domain parameters and to prevent related attacks [13,14].

3.1 Initial Setup

All entities involved in the protocol share the public quantities p, q, g where:

- p is the modulus, a prime number of the order 1024 bits or more.
- q is a prime number in the range of 159-160 bits, such that $q|(p-1)$.
- g is a generator of order q, where $\forall i < q, g^i \neq 1 \mod p$.
- Each entity has its own public key and private key pair ($\texttt{PK}_i$,$\texttt{SK}_i$), where $\texttt{PK}_i = g^{(\texttt{SK}_i)} \mod p$
- Entity i's public key ($\texttt{PK}_i$) is certified by its root certification authority (j) and is represented as $\texttt{CERT}_j\langle \texttt{PK}_i, i\rangle$.
- Public parameters p, q, g used by an e-passport are also certified by its root certification authority.

3.2 Phase One - IS Authentication (ISA)

Step 1 ($\mathcal{IS}$)**:** When an e-passport is presented to an IS, the IS reads MRZ information using an MRZ reader and issues the smart card command GET CHALLENGE to the e-passport chip.

Step 2 ($\mathcal{C}$)**:** The e-passport chip then generates a random $c \in_R 1 \leq c \leq q-1$ and computes $K_c = g^c \mod p$, playing its part in the key agreement process to establish a session key. Chip replies to the GET CHALLENGE command by sending K_c and its domain parameters p, q, g.

$$\mathcal{C} \longrightarrow \mathcal{IS} : K_c, p, q, g$$

Step 3 ($\mathcal{IS}$)**:** On receiving the response from the chip, the IS generates a random $is \in_R 1 \leq is \leq q-1$ and computes its part of the session key as K_{is} $= g^{is} \mod p$. IS digitally signs the message containing MRZ value of the e-passport and K_c.

$$S_{\mathcal{IS}} = \mathtt{SIGN}_{\mathtt{SK}_{\mathcal{IS}}}\langle MRZ\|K_c\rangle$$

It then contacts the nearest DV of the e-passports issuing country and obtains its public key. IS encrypts and sends its signature $S_{\mathcal{IS}}$ along with e-passports MRZ information and K_c using DV's public key $\mathtt{PK}_{\mathcal{DV}}$.

$$\mathcal{IS} \longrightarrow \mathcal{DV} : \mathtt{ENC}_{\mathtt{PK}_{\mathcal{DV}}}\langle S_{\mathcal{IS}}, MRZ, K_c\rangle, \mathtt{CERT}_{\mathcal{CVCA}}\langle \mathtt{PK}_{\mathcal{IS}}, \mathcal{IS}\rangle$$

Step 4 ($\mathcal{DV}$)**:** DV decrypts the message received from IS and verifies $\mathtt{CERT}_{\mathcal{CVCA}}\langle \mathtt{PK}_{\mathcal{IS}}, \mathcal{IS}\rangle$ and the signature $S_{\mathcal{IS}}$. If the verification holds, DV knows that IS is genuine and creates a digitally signed message $S_{\mathcal{DV}}$ to prove IS's authenticity to the e-passport.

$$S_{\mathcal{DV}} = \mathtt{SIGN}_{\mathtt{SK}_{\mathcal{DV}}}\langle MRZ\|K_c\|\mathtt{PK}_{\mathcal{IS}}\rangle, \mathtt{CERT}_{CVCA}\langle \mathtt{PK}_{\mathcal{DV}}, \mathcal{DV}\rangle$$

DV encrypts and sends the signature $S_{\mathcal{DV}}$ using the public key $\mathtt{PK}_{\mathcal{IS}}$ of IS.

$$\mathcal{DV} \longrightarrow \mathcal{IS} : \mathtt{ENC}_{\mathtt{PK}_{\mathcal{IS}}}\langle S_{\mathcal{DV}}, [\mathtt{PK}_{Chip}]\rangle$$

DV may choose to send the public key of the chip if required. This has an obvious advantage, because the IS system now trusts DV to be genuine, it can obtain a copy of e-passport chip's PK to verify during E-passport authentication.

Step 5 ($\mathcal{IS}$)**:** IS on decrypting the message received, computes the session key $K_{cis} = (K_c)^{is}$ and encrypts the signature received from DV, the e-passport MRZ information and K_c using K_{cis}. It also digitally signs its part of the session key K_{is}.

$$\mathcal{IS} \longrightarrow \mathcal{C} : K_{is}, \mathtt{SIGN}_{\mathtt{SK}_{\mathcal{IS}}}\langle K_{is}, p, q, g\rangle, \mathtt{ENC}_{K_{cis}}\langle S_{\mathcal{DV}}, MRZ, K_c\rangle$$

Step 6 $\mathcal{C}$**:** The chip on receiving the message from IS computes the session key $K_{cis} = (K_{is})^c$. It decrypts the message received using the session key and verifies signature $S_{\mathcal{DV}}$ and $\mathtt{VERIFY}_{PK_{\mathcal{IS}}}\langle \mathtt{SIGN}_{\mathtt{SK}_{\mathcal{IS}}}\langle K_{is}, p, q, g\rangle\rangle$. On successful verification, the chip is convinced that the IS system is genuine and can proceed further in releasing its details. All further communication between an e-passport and IS is encrypted using the session key K_{cis}

3.3 Phase Two - E-Passport Authentication (EPA)

Step 1 $\mathcal{C}$**:** The IS issues an INTERNAL AUTHENTICATE command to the e-passport. The e-passport on receiving the command creates a signature $S_{\mathcal{C}}$ $= \mathtt{SIGN}_{\mathtt{SK}_{chip}}\langle MRZ\|K_{cis}\rangle$ and sends its domain parameter certificate to IS. The entire message is encrypted using the session key K_{cis}.

$$\mathcal{C} \longrightarrow \mathcal{IS} : \mathtt{ENC}_{K_{cis}}\langle S_{\mathcal{C}}, \mathtt{CERT}_{DV}\langle \mathtt{PK}_{\mathcal{C}}\rangle, \mathtt{CERT}_{DV}\langle p, q, g\rangle\rangle$$

Step 2 ($\mathcal{IS}$)**:** IS decrypts the message and verifies $\mathtt{CERT}_{DV}\langle p, q, g\rangle$, $\mathtt{CERT}_{DV}\langle \mathtt{PK}_{\mathcal{C}}\rangle$ and $S_{\mathcal{C}}$. If all three verification holds then IS is convinced that the e-passport is genuine and authentic.

During ISA, IS sends the e-passports MRZ information to the nearest e-passport's DV, which could be an e-passport country's embassy. Embassies are DV's as they are allowed to issue e-passport to their citizens and as most embassies are located within an IS's home country, network connection issues will be minimal.

Sending MRZ information is also advantageous, as the embassy now has a list of all its citizens who have passed through a visiting country's border security checkpoint. We do not see any privacy implications, because, most countries require their citizen to register at embassies when they are visiting a foreign country.

4 Analysis of E-Passport Scheme

In this section we identify important security goals required in an e-passport protocol and perform a security analysis of our proposed OSEP protocol.

4.1 Requirement Analysis

The two most important requirements for border security are,:identification of the passport bearer and authentication of the passport data. Due to the digital nature of data stored in an e-passport, it is easy for the data to be copied or modified. An e-passport protocol will need to address security requirements that will affect electronic data storage and transmission. The references [9,1] provided a brief overview of security goals for e-passports. The description in the references was limited and did not consider goals that are essential in the analysis of cryptographic protocols. Our security goals for an e-passport system are:

Goal 1 *Identification*: After a successful completion of an e-passport protocol, both an e-passport and IS must obtain guarantees (unforgeable proof) of the other party's identity.

Goal 2 *Authenticity*: After a successful completion of an e-passport protocol, both an e-passport and IS must be sure about authenticity of messages received during the conversation with each other, and should also have an undeniable proof of the origin of messages.

Goal 3 *Data confidentiality*: Data confidentiality during an e-passport protocol run is guaranteed by the security of session key agreed between an e-passport and IS, therefore, if the e-passport completes a single protocol run with the view that it has negotiated a session key K with IS, then the e-passport is guaranteed that no other third-party has learnt key K and if IS completes the protocol run then it associates the key K with the e-passport. Data confidentiality of information stored in the e-passport chip is not considered as it is protocol independent, but is necessary for an e-passport protocol to detect if information was tampered, which is provided by our integrity goal.

Goal 4 *Integrity*: Integrity of data in an e-passport chip is guaranteed by signatures, therefore, in a run of an e-passport protocol, if an IS successfully verifies and validates signatures on messages from the e-passport, then the

IS obtains guarantee about information held in the e-passport chip has not been modified by any third party or the e-passport bearer after chip's initialisation by DS.

Goal 5 *Privacy*: In every run of an e-passport protocol, the e-passport bearer is assured that, his/her e-passport's digital identity is revealed only to an authenticated IS involved in the current protocol run.

Goal 6 *Session key security*: Both entities, an e-passport and IS have proof that, each run of the e-passport protocol is unique and compromise of long term keys does not compromise session keys derived in the previous protocol runs.

4.2 Security Analysis of the OSEP Protocol

In this section we present a brief security analysis of the OSEP protocol. We first list our assumptions and then our claims about the OSEP protocol's security that corresponds to our security goals described in Section §4.1.

Assumptions

- In the OSEP protocol both an e-passport and IS instantiate a non-concurrent protocol run (session) between them, whereas session connections between IS and DV may run concurrently.
- IS is always the initiator of a protocol run and an e-passport is always the responder.
- The underlying security for Diffie-Hellman (DH) key exchange, the Decisional Diffie-Hellman (DDH) assumption holds.
- Cryptographic primitives like, symmetric and public key encryption, digital signatures, message authentication codes and hash functions are secure under the standard security notions.

Lemma 1. *If the encryption scheme used in the protocol is secure against the CCA2 attack then at the end of the OSEP protocol, both $\mathcal{C}$ and $\mathcal{IS}$ will complete matching sessions and get the same session key.*

Proof (Sketch)*:* Since the signature algorithm is secure against existential forgery under the adaptive chosen-message attack (by assumption), the MRZ information along with randomness of K_c and K_{is} guarantees the freshness of the message and binds the message with the two communicating parties. Therefore an attacker cannot forge or modify a message. For an attacker to forge or modify a message that is acceptable by $\mathcal{IS}$ or $\mathcal{C}$, he would need to forge the signature on $\mathtt{SIGN}_{\mathtt{SK}_{IS}}\langle K_i, p, q, g\rangle$ in phase 1, step 5 or forge the signature on $S_{\mathcal{C}}$ in phase 2, step 1. This contradicts our assumptions.

Furthermore, the digital signature by $\mathcal{C}$ contains the freshly generated session key K_{cis}. This prevents replay of messages from a previous run by an adversary who is not able to to generate signatures on both K_c and K_{cis}. □

Theorem 1. *The protocol provided in Section 3 is SK-secure if the encryption scheme used is secure against the CCA2 attack.*

Proof. In order to prove our protocol is SK-secure [15], we have to prove that $\mathcal{C}$ and $\mathcal{IS}$ get the same session key after they complete matching sessions and that an adversary cannot distinguish the session key K_{cis} from a random value with a non-negligible advantage. The former directly follows Lemma 1 and the following lemma provides proof for later.

Lemma 2. *Assuming DDH and the signature scheme is secure, then an attacker cannot distinguish the session key K_{cis} from a random value with a non-negligible advantage.*

Proof (Sketch)*:* The proof is by contradiction. Lets assume that an attacker can distinguish the session key K_{cis} from a random value with a non-negligible advantage η. In the C-K model [15], the key exchange attacker is not permitted to corrupt the *test session* or its *matching session*, so an attacker cannot directly get the session key K_{cis} from an attack on the OSEP protocol. Therefore, the attacker has two possible method to distinguish K_{cis} from a random value.

- The attacker learns the session key K_{cis}.
- The attacker successfully establishes a session (other than a test or its matching session) that has the same session key as the test session.

The first methods means that given g, g^c, g^{is}, g^α, the attacker is able to distinguish $\alpha = K_{cis}$ from random. This contradicts our DDH assumption. For the second method, there are two strategies an attacker can take. (A) After $\mathcal{C}$ and $\mathcal{IS}$ complete the *matching sessions*, the attacker establishes a new session with either $\mathcal{C}$ or $\mathcal{IS}$. But this session key will be not the same as K_{cis} as the values c and is are chosen randomly by $\mathcal{C}$ or $\mathcal{IS}$. (B) The attacker intervenes during the run of the protocol and makes $\mathcal{C}$ and $\mathcal{IS}$ get the same session key but not complete *matching sessions*. But this is not feasible according to Lemma 1 and we know that an attacker cannot succeed. □

Thus from Lemma 1 and Lemma 2, we know that $\mathcal{C}$ and $\mathcal{IS}$ will get the same session key after the completion of matching sessions and the attacker cannot distinguish the session key from a random value with a non-negligible advantage. In accordance with definition of SK-security [15](Definition 1) the OSEP is SK-secure.

Theorem 2. *The OSEP protocol provides undeniable proof of identification of both $\mathcal{C}$ and $\mathcal{IS}$.*

Proof (Sketch)*:* The message sent to $\mathcal{C}$ by $\mathcal{IS}$ in Step 5 of ISA includes the values, $S_{\mathcal{DV}}$, MRZ and K_c. The signed message $S_{\mathcal{DV}}$ contains public key of $\mathcal{IS}$ verified by $\mathcal{DV}$, so it is sufficient for $\mathcal{C}$ to verify $S_{\mathcal{DV}}$ to successfully identify $\mathcal{IS}$ as genuine.

An adversary wishing to falsely identify of IS will need to forge $S_{\mathcal{DV}}$. $S_{\mathcal{DV}}$ can be only generated with a valid DV's secret key ($\mathtt{SK}_{\mathcal{DV}}$). The adversary cannot forge $S_{\mathcal{DV}}$ as he does not know $\mathtt{SK}_{\mathcal{DV}}$.

An adversary who does not have K_{cis} and $\mathtt{SK}_{C}$, will not be able to identify as a genuine $\mathcal{C}$, because, in EPA $\mathcal{C}$ is required to digitally sign its MRZ and the freshly generated session key K_{cis}. Therefore, the OSEP protocol provides non-repudiable proof of identity for both $\mathcal{IS}$ and $\mathcal{C}$. □

Remark 1. The strict privacy requirement is, the e-passport protocol guarantees no information about an e-passport bearer is available to any unauthorised entities and the relaxed privacy requirement is, when the e-passport protocol guarantees that digital identity or biometric information of an e-passport bearer is not be available to any unauthorised entities. The OSEP protocol provides partial forward secrecy under the strict privacy requirement as loss of the long-term secret key of both $\mathcal{IS}$ and $\mathcal{DV}$ will reveal the MRZ information of an e-passport. But, compromise of long term key does not compromise the previous session keys established. Also, any loss of session key in the previous protocol does not compromise future runs of an e-passport protocol. Thus under the relaxed privacy requirement, the OSEP protocol provides perfect forward secrecy.

In addition, in the OSEP protocol, an e-passport bearer is sure about protection of his/her digital identity against an unauthenticated $\mathcal{IS}$ and *unknown adversaries* as the digital identity of an e-passport bearer $\mathtt{PK}_{\mathcal{C}}$ is revealed only in the step one of EPA. EPA follows a successful ISA, therefore $\mathcal{C}$ is also sure about the $\mathcal{IS}$ identity. The digital identity is also protected from any adversary eavesdropping on the communication as it is encrypted using the fresh secure session key established during ISA.

The OSEP protocol also provides tamper detectable integrity check for data in an e-passport's chip. Integrity of e-passport data provided in OSEP is similar to what was provided by both first generation and second generation passports. The data stored in an e-passport's chip is hashed and digitally signed by the e-passport's DS at the time of initialisation. Therefore as a consequence of the assumption four, that hash functions and digital signatures are secure, the OSEP protocol provides integrity verification. An adversary wishing to authenticate modified data will need to forge the digital signature of DS on the hash values. This is infeasible as the adversary does not know the DS's private key $\mathtt{SK}_{\mathcal{DS}}$.

To summarise, OSEP is a simple and efficient protocol. Its main advantages are that it not only protects the chip's data during communication from an eavesdropper, but also restricts access to an unauthenticated IS. The protocol requires very little modification to existing PKI implemented by the first generation e-passport standard. A disadvantage of the OSEP protocol is, its on-line nature of authentication mechanism. IS is required to contact the e-passport countries DV and authenticate itself before it can continue communication with an e-passport. This process might incur some delay, but we expect this delay to be minimal as the communication between IS and DV will be through a high-speed network.

5 Conclusion

Security techniques implemented in both the first and second generation of e-passports do not adequately protect an e-passport bearer. The first generation e-passport standard is vulnerable to brute force attacks because session keys generated have a very low entropy. The second generation e-passport proposal requires extensive modifications to exiting infrastructure and it still relies on the first generation standards to provide a secure connection to protect primary biometric identifiers. Both the standard have ignored the need to protect e-passports details during setting up a communication, which makes the e-passport bearer vulnerable to identity theft and covert surveillance.

We have presented an on-line e-passport protocol that addresses many weaknesses in both the first and second generation e-passport protocols. Our proposal also offers significant security advantages. The security measures will make an e-passport extremely hard for a malicious user to authenticate as a genuine e-passport bearer or as an IS. The proposed protocol also protects the details of an e-passport bearer from an unauthorised IS thus reducing the threat of identity theft. The OSEP protocol also uses existing PKI infrastructure in place for the first generation e-passport standard and eliminates the need for sending certificate chain as proposed in the second generation e-passport standard, making an e-passport in OSEP protocol less vulnerable to DOS based attacks. Electronic passports are an important step in the right direction. They enable countries to digitise their security at the border control and provide faster and safer processing of an e-passport bearer. The OSEP protocol strengthens this process by providing an enhanced e-passport security measure.

Acknowledgments

The work is supported by Australian Research Council grants DP0663452, DP0558773 and DP0665035.

References

1. ICAO: Machine readable travel documents. Technical report, ICAO (2006)
2. ISO/IEC: Iso/iec14443, identification cards – contactless integrated circuit(s) cards – proximity cards (2000)
3. Juels, A., Molnar, D., Wagner, D.: Security and privacy issues in e-passports. In: IEEE SecureComm. 2005 (2005)
4. Laurie, A.: Rfidiot (2007)
5. Australian Customs Service: Smartgate (2006)
6. Kc, G.S., Karger, P.A.: Preventing attacks on machine readable travel documents (mrtds) (2005), http://eprint.iacr.org/
7. Pasupathinathan, V., Pieprzyk, J., Wang, H.: Formal analysis of icao's e-passport specification. In: Brankovic, L., Miller, M. (eds.) Australasian Information Security Conference (AISC2008). Conferences in Research and Practice in Information Technology (CRPIT), vol. 81, Australian Computer Society (2008)

8. Justice and Home Affairs: Eu standard specifications for security features and biometrics in passports and travel documents. Technical report, European Union (2006)
9. Kügler, D.: Security concept of the eu-passport. Security in Pervasive Computing 85 (2005)
10. Kügler, D.: Adavance security mechanisms for machine readable travel documents. Technical report, Federal Office for Information Security (BSI), Germany (2005)
11. Desmedt, Y., Goutier, C., Bengio, S.: Special uses and abuses of the fiat-shamir passport protocol. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 21–39. Springer, Heidelberg (1988)
12. Scherzer, H., Canetti, R., Karger, P.A., Krawczyk, H., Rabin, T., Toll, D.C.: Authenticating mandatory access controls and preserving privacy for a high-assurance smart card. In: Snekkenes, E., Gollmann, D. (eds.) ESORICS 2003. LNCS, vol. 2808, pp. 181–200. Springer, Heidelberg (2003)
13. Wiemers, A.: Kommentare zu application interface for smart cards used as secure signature creation device, part 1 - basic requirements. Technical Report Version 0.14, Bonn, Germany (2003)
14. ANSI: Public key cryptography for the financial services industry, key aggreement and key transport using elliptic curve cryptography. Technical report, American National Standards Institute (ANSI 2001) (2001)
15. Canetti, R., Krawczyk, H.: Analysis of key exchange protocols and their use for building secure channels. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 453–474. Springer, Heidelberg (2001)

A Basic Access Control and Passive Authentication

Basic access control is an optional security mechanism that uses ISO 11770-2 *Key Establishment Mechanism 6* to form a secure channel between IS and a chip. The protocol uses two secret keys (K_{ENC}, K_{MAC}) that are stored in a chip. IS derives both these keys using scanable data present in MRZ, namely passport number, date of birth of the passport bearer, date of passport validity and check digits for those values. The three pass challenge-response protocol is initiated by IS which requests a challenge from the chip. On receiving the challenge (Rnd_{C2}) IS creates a checksum according to ISO/IEC 9797-1 *MAC algorithm 3* over the cipher text that contains IS's response to chip's challenge Rnd_{R2} and keying material K_R. The chip on obtaining IS's response creates a checksum that includes its keying material K_C. Both IS and the chip verify the MAC obtained and decrypt the message to reveal both keying materials, to form the "key seed" K_{seed}. K_{seed} is used to derive a shared session key using the key derivation algorithm described in [1] (*Appendix 5*). Passive authentication (PA) provides only a basic level of security, as it is still vulnerable to skimming and eavesdropping attacks. PA is used to verify the integrity and to authenticate data stored in an e-passport. The e-passport bearer information is digitally signed by DS (Documemnt Signer) and verified by IS during PA.

Chip		**IS**
$Rnd_{C2} \in_R \{0,1\}^{64}$		
	$\xrightarrow{Rnd_{C2}}$	
		$Rnd_{R2}, K_R \in_R \{0,1\}^{64}$
		$S = Rnd_{R2} \| Rnd_{C2} \| K_R$
		$E_R = ENC_K\{S\}, M_R = MAC_{K_M}\{E_R\}$
	$\xleftarrow{E_R \| M_R}$	
Verify M_R,Decrypt E_R		
Verify Rnd_{C2},$K_C \in_R \{0,1\}^{64}$		
$R = Rnd_{C2} \| Rnd_{R2} \| K_C$		
$E_C = ENC_K\{R\}, M_C = MAC_{K_M}\{E_C\}$		
	$\xrightarrow{E_C \| M_C}$	
$K_{seed} = K_C \oplus K_R$		$DEC_K\{E_C\}$,Verify Rnd_{R2},$VMAC_{K_M}\{M_C\}$
		$K_{seed} = K_R \oplus K_C$
	$\xrightarrow{SO_D, LDS, C_{DS}}$	
		Obtain KPu_{DS},and KPu_{CSCA}
		Verify SO_D,C_{DS},Calculate H'_{LDS}
		$H'_{LDS} \overset{?}{=} H_{SO_D}$

Fig. 4. Basic Access Control and Passive Authentication