A Survey on the Evolution of Cryptographic Protocols in ePassports

Rishab Nithyanand

University of California - Irvine
rishabn@uci.edu

Abstract. ePassports are biometric identification documents that contain RFID Tags and are primarily used for border security. The embedded RFID Tags are capable of storing data, performing low cost computations and cryptography, and communicating wirelessly. Since 2004, we have witnessed the development and widespread deployment of three generations of electronic passports - The ICAO First Generation ePassport (2004), Extended Access Control (EAC v1.0) ePassports (2006), and Extended Access Control with Password Authentication and Connection Establishment (EAC v2.1) ePassports (2008). Currently, over thirty million ePassports have been issued around the world. In this paper, we provide an introductory study of the technologies implemented in ePassports - Biometrics, RFID, and Public Key Infrastructures; and then go on to analyze the protocols implemented in each of the three generations of ePassports, finally we point out their shortcomings and scope for future related research.

1 Introduction

An electronic passport (ePassport) is an identification document which possesses relevant biographic and biometric information of its bearer. It also has embedded in it a Radio Frequency Identification (RFID) Tag which is capable of cryptographic functionality. The successful implementation of Biometric and RFID technologies in documents such as ePassports aim to strengthen border security by reducing forgery and establishing without doubt the identity of the documents' bearer.

RFID enabled passports were first adopted by Malaysia in 1998 [1]. However, until 2002, these passports failed to maintain basic security requirements since the passport holder information was not encrypted. The only security measure that was implemented was a digital signature on all the data to ensure that information could not be modified by adversaries. This was largely inadequate since it did not prevent passports from being cloned, or illegal data gathering through passport skimming.

Later in 2004, as a guideline, the International Civil Aviation Organization issued a set of design guidelines and protocol specifications for nations that wished to implement RFID enabled passports. This was done in an attempt to standardize passport design while making them more secure. The security goals of the ICAOs ePassport specifications were identified as: Data Confidentiality, Data Integrity, Data Origin Authentication, Non Repudiation, Mutual Authentication, and Key Integrity.

Soon after the ICAO released their ePassport specifications, the first major initiative towards the global implementation of ePassports for increased border security was taken by the United States in 2006. It mandated the adoption of the ICAO specification by the twenty-seven nations in its Visa Waiver Program (VWP) [2]. As the US goverment pushed for the global adoption of ICAO's ePassport standards, evidence of inadequate data protection aroused media attention and public concern [3]. As a result of these concerns, a new specification which

included a set of protocols called Extended Access Control (EAC) that mitigated some of the privacy issues in the first generation of ePassports was proposed in 2006 [4]. The EAC protocol stack introduced the concept of mutual authentication which allowed the authentication of a Tag and Reader to each other. After its release, there were several proposals for the third generation ePassport scheme which included authentication protocols such as OSEP (Online Secure ePassport Protocol [5]) and an online authentication mechanism based on the Elliptic Curve Diffie-Hellman key agreement [6].
Finally, in October 2008 a new protocol stack was released by the Bundesamt fur Sicherheit in der Informationstechnik (BSI) - Germany called EAC v2.1. This protocol introduced a new version of Tag and Reader authentication which fixed some issues present in the original EAC proposal. In addition, a new protocol called Password Authenticated Connection Establishment (PACE) was added to the EAC protocol stack. This protocol aimed to further improve security through stronger user authentication.

1.1 Contributions

Through this paper we provide an introduction to the three constituent technologies in ePassports - Biometrics, Public Key Infrastructure, and RFID. We also effectively summarize the contents of three technical reports which describe the protocols and the functioning of the ICAO first generation ePassport specifications [7], the EAC ePassport specifications [8], and the EAC v2.1 ePassport specifications [9]. This is the first work that analyses the protocols behind the third generation ePassport. We also present some feasible threats to the EAC v2.1 protocol.

1.2 Related Work

RFID Security, Privacy, and Authentication: The implications of large scale infiltration of RFID Tags in the consumer market on security and privacy of individuals was first considered in [10, 11]. Since then there has been work in the area of developing security measures for EPC Tags (Electronic Product Code) which use RFID to replace barcodes for inventorying and product identification. These include anti-cloning protocols [12–14], cryptographic tools and protocols for use in EPCs and other low power Tags [15], authentication protocols [16, 17], and protocols to prevent anauthorized tracking of EPC Tags [18]. Many of these are applicable even to ePassports, eIDs, and ePassport cards [19].

ePassport Security : Juels *et al.* presented the first analysis of the security of the cryptographic protocols used in first generation ePassports in [20]. This work was followed by [21], which illustrated some hypothetical scenarios that could cause a compromise in security and privacy of the holders of first generation ePassports and eIDs. Carluccio *et al.* presented some unique tracking attacks on the first generation ePassport in [22].
Soon after the EAC specifications for second generation ePassport were released, its vulnerabilities were exposed, and a new ePassport protocol - OSEP was proposed in [5]. Other researchers exposed the weaknesses of the ePassport implementation in Europe [23]. In other work, Lekkas and Gritzalis studied the possibility of extending the ePassport PKI to other applications such as POS and online transactions [24]. Recently, Kalman and Noll analysed the feasibility of implementing watermarking technologies on ePassports to prevent biometric data leakage [25].

1.3 Organization

In section 2, we provide a brief introduction to Biometrics, Public Key Infrastructures (PKIs), and RFIDs. In section 3, we describe the Logical data Structure (LDS) in ePassports, introduce the ICAO 14443 specification and their implications on ePassport communication, and derive a power-distance relationship for ePassports. In section 4, we describe the cryptographic protocols behind the first generation ePassport and its operation procedure. In section 5 and 6, we do the same for the second and third generation ePassports respectively. In section 7, we go over the vulnerabilities of each generation of ePassports and describe some attacks that are still feasible even with EAC v2.1 ePassports. Finally in section 8, we make our conclusions and discuss some future avenues for research.

2 ePassport Technologies

Electronic passports incorporate three technologies to help deal with user authentication and fraud management problems: Biometrics, Public Key Infrastructures (PKI), and Radio Frequency Identification (RFID). In this section we will provide a brief description of these technologies.

2.1 Biometrics

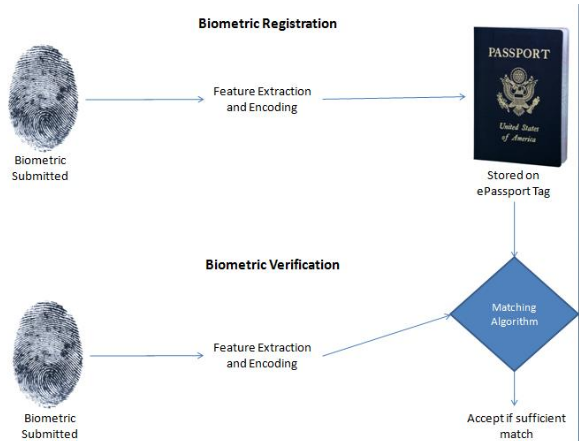


Fig. 1. Biometric Registration and Verification

A Biometric is a measurable physiological or behavioural trait that can be used to identify or verify the identity of an individual. Biometric Authentication is the process of authenticating individuals to computers using biological or physiological characteristics. They are fast becoming the prefered technique for user authentication in personal devices such as phones, laptops, etc. This may be attributed towards their resistance to forgery.

Commonly used biometrics include head shots, fingerprints, palm-prints, iris images, thermograms, hand geometry, retinal scans, DNA, and voice. ePassports favor the use of fingerprints as the primary biometric. The choice of the most effective biometric for an application is based on certain characteristics such as - Universality, Uniqueness, Permanence, Performance, Collectability, Acceptability, and Circumvention. [26]

The Biometric authentication procedure for electronic passports involves two processes - Registration and Verification. During the registration phase, the ePassport applicant registers their biometric at a secure location under human supervision. A feature extraction program is used to encode this biometric data after which it is stored on the users ePassport Tag. For user authentication and identity verification at an inspection terminal, the user is made to supply a sample of their biometric. The same feature extraction algorithm is used to encode the freshly supplied biometric. A matching algorithm is run at the terminal to obtain the degree of similarity between the registered and supplied biometric. If the degree of similarity is deemed to be greater than a certain threshold value, the biometric is accepted and the user's identity is verified successfully.

Unfortunately, without human supervision, it is not always possible to detect the use of prosthetics at the biometric registration or verification stages. It is easy to see that biometric spoofing attacks will become easier to perform as automation increases and human supervision of the biometric process decreases.

2.2 Public Key Infrastructure (PKI)

A Public Key Infrastructure is required to aid the process of public key distribution and authentication. The Public Key Infrastructure for ePassports has remained unchanged over the last five years. The key elements in the ePassport PKI are the Country Verifying Certificate Authorities (CVCA) *a.k.a* Country Signing Certificate Authorities (CSCA), Document Verifiers (DV), and Inspection Systems (IS). The Public Key Infrastructure usually has a hierarchical structure. The highest level body in each nation acts as the CSCA. The CSCA generates and stores a key-pair (KPu_{CSCA}, KPr_{CSCA}). The private key of the CSCA (KPr_{CSCA}) is used to sign each Document Verifier (DV) certificate (from its own and from other countries). There are usually many Document Verifiers in each nation. Each of these Document Verifiers generates and stores a key-pair (KPu_{DV} , KPr_{DV}). The private key (KPr_{DV}) of the DV is used to sign each Inspection System (Reader) (IS) certificate in its domain and also the security data element (SOD) of every passport it issues. In order to efficiently share DV certificates from all nations, the ICAO provides a Public Key Directory (PKD). The PKD will store only the certificates of all registered DV's. This repository of certificates is available to every nation and is not read protected. Certificate Revocation Lists (CRL) may also be stored in the same PKD. Every nation is responsible for updating its own repository of public certificates and CRL's by downloading them from the PKD, once this is done, each nation distributes the newly downloaded information to every DV and IS in its jurisdiction.

2.3 Radio Frequency Identification

RFID is a wireless technology used for communication between a Tag and an inspection system called a Reader. Over the last few years, RFID technology has been an area of great controversy after it was implemented by some retail giants such as Benetton (Italy) and Metro Future Store (Germany) for undisclosed reasons. Since then there have been major protests and even product boycotts by privacy activists who fear that these RFID Tags are

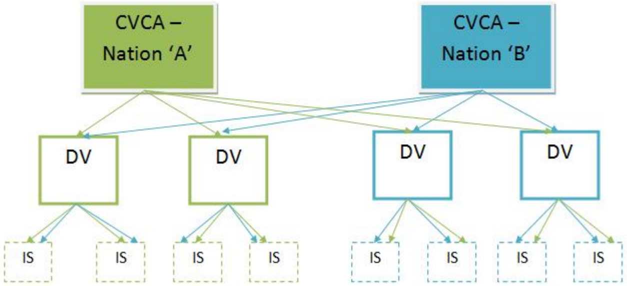


Fig. 2. ePassport Public Key Infrastructure

being used for activities such as behavior profiling and customer tracking [27]. Some of the major threats that need to be addressed when implementing RFID technology in sensitive fields such as international security are Scanning, Tracking, Eavesdropping, and Cloning *.i.e.* it is important that an adversary is unable to do the following:

- Read data from the Tag without consent of the passport holder.
- Track the movements of a passport holder.
- Eavesdrop on legitimate interactions.
- Build a new Tag that can be bound to a passport.

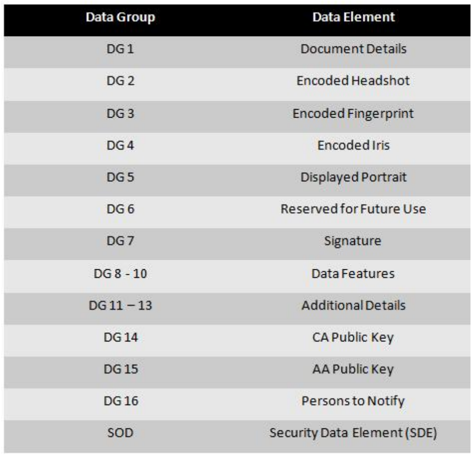
RFID consists of three subsystems: Tags, Readers, and antennas. RFID Tags can be one of three types: active, semi-active or passive. Active tags are those which are run by a battery, while passive tags have no batteries and use power obtained from radio signals emitted by the RFID Readers to operate. RFID Readers operate at a range of frequencies, power, and reading ranges; these characteristics are defined by the application. Antennas are usually built into the RFID Reader and the RFID Tag.

3 ePassport Standard Specifications

The ePassport has embedded in it an RFID Tag which is capable of cryptographic computations and is passive in nature. Passive RFID Tags were chosen because of their low cost, high fidelity, and short read ranges. The RFID system implemented in ePassports follow the ISO 14443 standard, which specifies the use of 13.56MHz radio frequencies for communication. The physical features of ePassport Tags are defined by the ISO 7810 ID-3 standard which specifies a Tag of size 125mm x 88mm. These RFID Tags have an antenna built around them. ePassport Tags have between 32 to 144 kilobytes of EEPROM memory built into them. In this memory we store 16 data groups ranging from DG1 - DG 16. These 16 groups store information such as data present on the Machine Readable Zone (MRZ) of the passport, extracted biometric features, public keys and other data items. Since ePassport RFID systems operate at 13.56MHz (HF), designing loop or dipole antennas that can be used on smart-cards and ePassports are not possible, instead we use the properties of inductive coupling for signal propagation between RFID Tags and Readers. There are many other challenges that also need to be addressed when designing RFID systems using passive HF Tags, these are explained by Gilles Cerede in [28].

3.1 ePassport Logical Data Structure

The ICAO issued a standardized data structure called Logical Data Structure (LDS) for the storage of data elements. This was to ensure that global interoperability for ePassport Tags and Readers could be maintained. The specifications state that all the 16 data groups are write protected and can be written only at the time of issue of the ePassport by the issuing state. A hash of data groups 1-15 are stored in the security data element (SOD), each of these hashes should be signed by the issuing state.



Data Group	Data Element
DG 1	Document Details
DG 2	Encoded Headshot
DG 3	Encoded Fingerprint
DG 4	Encoded Iris
DG 5	Displayed Portrait
DG 6	Reserved for Future Use
DG 7	Signature
DG 8 - 10	Data Features
DG 11 – 13	Additional Details
DG 14	CA Public Key
DG 15	AA Public Key
DG 16	Persons to Notify
SOD	Security Data Element (SDE)

Fig. 3. ePassport Logical Data Structure

3.2 Power-Distance relation for ePassport Tags

We make use of inductive coupling to transfer power from the Reader to the Tag. In this circuit,V_0 represents the voltage supply source of the Reader which has an internal resistance R_0. We use a coil with inductance L_1 as the Readers' antenna. The antenna is matched with the voltage source using the two capacitors C_s and C_p. We couple this circuit with the Tag equivalent circuit in which L_2 is the Tag antenna inductance and capacitor C_2 along with L_2 completes the resonant circuit. The remaining equipment on the Tag can be represented as the load resistance R_L. The power required by the ePassport RFID Tags supplied to many nations by *Infineon Technologies* to operate is 55mW [29].

We first establish the relationship between mutual inductance and distance between the antennas of the Reader and Tag with (2)

$$M = \frac{\mu_r \pi N_1 N_2 (r_1)^2 (r_2)^2}{2\sqrt{((r_1)^2 + x^2)^3}} = \frac{1.57 \times 10^{-12}}{x^3} \tag{1}$$

Where μ_r represents Permeability; 'N_1' and 'N_2' are the number of turns in the antennas of the Reader and Tag; 'r_1' and 'r_2' represent the radii of the coils (antennas) of the Reader and Tag circuits and 'x' is Distance between the Reader and Tag. At resonance, a Reader running with current I_1 will induce power in the amount of P_{Tag} in the Tag circuit.

$$P_{Tag} = (I_1)^2 R_T \tag{2}$$

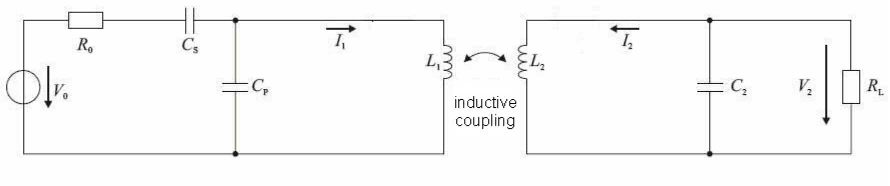


Fig. 4. HF RFID Equivalent Circuit

Where R_T is the Tag impedence given by the following relation:

$$R_T = \frac{M^2 R_L}{(L_2)^2} \tag{3}$$

Where R_L is the load resistance and can be calculated using the relation $R_L = (V_T)^2/P_{Tag}$. Now, Substituting R_T and M in (3), we obtain

$$P_{Tag} = \frac{(I_1)^2 M^2 R_L}{(L_2)^2} \tag{4}$$

Assuming that the Tag requires 55mW for operation and has a Load Resistance of 550Ω, we get $x = 9.8$ centimeters. From the above equations, we can conclude that for inductively coupled HF RFIDs, $P_{Tag} \propto M^2$ and M$\propto \frac{1}{x^3}$.

4 First Generation ePassports

In 2004, the International Civil Aviation Organization (ICAO) published a set of guidelines (in Doc 9303) that were meant to be followed as the *de-facto* ePassport standard. The default mandatory biometric to be used is the headshot of the individual, other allowable biometrics are fingerprints and iris images. There are three Cryptographic protocols described in the first generation ICAO specifications to ensure data correctness and privacy. These are Passive Authentication, Basic Access Control, and Active Authentication.

4.1 Passive Authentication

Passive Authentication is the only mandatory cryptographic protocol in the ICAO first generation specification. Its primary goal is to allow a Reader to verify that the data in the ePassport is authentic. This scheme is known as passive authentication since the Tag performs no processing and is only passively involved in the protocol. One must note that Passive Authentication does not tie the Tag to a passport *i.e.* we can only establish that the data on the Tag is correct, not the authenticity of the Tag itself (it cannot detect cloning).

The Inspection System retreives the certificate of the issuing document verifier, using the public key from the certificate it verifies the digital signature used to sign the data in the LDS. Once the validity of the signature is established, the Reader computes the hash of each of these data elements and compares them with the hashed values stored in the SOD. If there is a match, it can be established that the data on the Tag was not manipulated.

4.2 Active Authentication

Active Authentication is an optional protocol in the ICAO first generation specifications. Using a simple challenge-response mechanism, it aims to detect if a Tag has been substituted or cloned. If Active Authentication is supported, the Tag on the ePassport stores a public key (KPu_{AA}) in Data Group 15 and its hash representation in the SOD. The corresponding private key (KPr_{AA}) is stored in the secure section of Tag memory. In order for the Tag to establish its authenticity, it must prove to the Reader that it posseses this private key.

1. The Reader sends a randomly generated 64 bit string (R) to the Tag.
2. The Tag signs this string using the key KPr_{AA} and sends this signature to the Reader.
3. The Reader obtains the public key KPu_{AA} stored in Data Group 15.
4. The Reader verifies the correctness of the signed string using its knowledge of R and KPu_{AA}.

4.3 Basic Access Control

Basic Access Control (BAC) is an optional protocol that *tries* to ensure that only Readers with physical access to the passport can read Tag data. When a reader attempts to scan the BAC enabled ePassport, it engages in a protocol which requires the Reader to prove knowledge of a pair of secret keys (called 'access keys') that are derived from data on the Machine Readable Zone (MRZ) of the passport. From these keys, a session key which is used for secure messaging is obtained.

The Access Keys (K_{ENC}, K_{MAC}) are derived from the following data available on the MRZ: The Passport Number (Doc No), Date of Birth of the Passport Holder (DOB), Valid Until Date of the Passport (DOE), 3 Check Digits (C).

$$K_{seed} = 128msb(SHA - 1(DocNo||DOB||DOE||C))$$
$$K_{ENC} = 128msb(SHA - 1(K_{seed}||1))$$
$$K_{MAC} = 128msb(SHA - 1(K_{seed}||2))$$

The Reader will now enter a Challenge-Response mechanism (described below) to prove possession of the access keys and to derive a session key.

1. The Tag generates and sends the Reader a 64 bit string (R_T).
2. The Reader receives R_T and generates two random 64 bit strings (R_R, K_R).
3. The Reader now encrypts $R_R||R_T||K_R$ using the 3-DES algorithm and the key K_{ENC}.
4. The Reader now computes the MAC of the cipher using ANSI MAC with the key K_{MAC}.
5. The Reader sends the cipher and the MAC to the Tag.
6. The Tag checks the MAC, decrypts the cipher. It verifies the correctness of R_T and then extracts K_R.
7. The Tag generates another 64 bit random string K_T.
8. The Tag now encrypts $R_T||R_R||K_T$ using the 3-DES algorithm and K_{ENC}.
9. The Tag now computes the MAC of the cipher using ANSI MAC with the key K_{MAC}.
10. The Tag sends the cipher and the MAC to the Reader.
11. The Reader checks the MAC, decrypts the cipher. It verifies the correctness of R_R and then extracts K_T.
12. Both the Reader and the Tag compute the session key seed (K_{seed}) as $K_R \oplus K_T$.

Now both parties generate a new session encryption key K_E and a session MAC key K_M as shown below.

$$K_E = 128msb(SHA - 1(K_{seed}||1))$$
$$K_M = 128msb(SHA - 1(K_{seed}||2))$$

From this point on all communication is secured using the above encryption and MAC keys.

5 Second Generation ePassports

In 2006 a new set of standards for electronic passports called Extended Access Control was approved by the New Technologies Working Group (NTWG) which was based on the proposal for ePassport standardization made by the European Union. The primary goal of EAC was to provide more comprehensive Tag and Reader authentication protocols. It also aimed to promote the implementation of secondary biometrics for additional security. In this section we will describe the Chip Authentication and Terminal Authentication protocols and some of the flaws that were not mitigated by its inception. To achieve mutual authentication, the EAC proposal introduced two new protocols called Chip Authentication and Terminal Authentication. These were used to supplement the Passive Authentication protocol, Basic Access Control protocol and possibly the Active Authentication protocol described in the ICAO first generation ePassport specifications.

5.1 Chip Authentication

The Chip Authentication protocol is a mandatory protocol in the EAC specifications. It aims to replace Active Authentication as a mechanism to detect cloned ePassports. If Chip Authentication is performed successfully it establishes a new pair of encryption and MAC keys to replace BAC derived session keys and enable secure messaging. It does this using the static Diffie-Hellman key agreement protocol. Note that the ePassport Tag already has a Chip Authentication public key (in Data Group 14) and private key (in secure memory) $(TKPu_{CA}, TKPr_{CA})$. The process of Chip Authentication is described below.

1. The Tag sends $TKPu_{CA}$ to the Reader along with the Diffie-Hellman key agreement parameters (D).
2. The Reader verifies the correctness of the received key using Passive Authentication (section 3.1.1).
3. The Reader uses the data in D to generate its own public and private key pair ($RKPu_{CA}$, $RKPr_{CA}$).
4. The Reader sends the generated public key $RKPu_{CA}$ to the Tag.
5. The Reader and Tag can now generate a new seed key (K_{seed}) using this shared information.
6. The new encryption and MAC keys are generated as described in section 3.1.3.

5.2 Terminal Authentication

The Terminal Authentication protocol is a protocol that is executed only if access to more sensitive data (secondary biometrics) is required. It is a challenge-response mechanism that allows the Tag to validate the Reader used in Chip Authentication. The Reader proves to the Tag using digital certificates that it has been authorized by the home and visiting nation to read ePassport Tags. The process of Terminal Authentication is described below.

1. The Reader sends the Tag an Inspection System certificate (which was received from the local DV) and the DV's certificate (which was received from the CVCA).
2. The Tag inspects the certificates and extracts the public key ($RKPu_{TA}$) of the Reader from the Inspection System certificate.
3. The Tag generates a random string (R) and sends it to the Reader.
4. The Reader computes the hash of $RKPu_{CA}$ derived in the Chip Authentication protocol.
5. The Reader signs the message (R||SHA-1($RKPu_{CA}$)) with its private key ($RKPr_{TA}$).
6. The Tag verifies the correctness of R and $RKPu_{CA}$ using the key $RKPu_{TA}$ and grants access to secondary biometrics accordingly.

6 Third Generation ePassports

In late 2008, the Federal Office for Information Security (BSI - Germany) released a document describing new security mechanisms for electronic passports. In this section we will describe these protocols third generation ePassports. While this specification is suitable for eSign, eID and ePassport applications, we will describe it only for its relevence to ePassports. The third generation specification introduces a new protocol called PACE. In addition to PACE, the Terminal Authentication and Chip Authentication protocols were also updated. The PACE (Password Authenticated Connenction Establishment) protocol is introduced as a replacement to the Basic Access Control mechanism.

6.1 Password Authenticated Connection Establishment(PACE)

PACE replaces the Basic Access Control protocol as a mechanism which enables a Tag to verify that the Reader has authorized access to the electronic passport. The Tag and the Reader share a common password (π) which is used in conjunction with the Diffie-Hellman key agreement protocol to provide a strong session key. The entire process is described below.

1. The Tag encrypts a random nonce (s) using the key K_{π}. Here, K_{π} is SHA-1(π||3).
2. The Tag sends the encrypted nonce and the Diffie Hellman key agreement static domain parameters (D) to the Reader.
3. The Reader uses the shared password (π) to recover the encrypted nonce (s).
4. The Tag and the Reader compute the Diffie-Hellman ephemeral key domain parameters (D') using D and s.
5. The Tag generates a key pair given by($PACEKPr_T$, $PACEKPu_T$) and sends $PACEKPu_T$.
6. The Reader generates the key pair ($PACEKPr_R$, $PACEKPu_R$) and sends $PACEKPu_R$.
7. The Reader and Tag now have enough shared information to generate a seed key (K_{seed}).
8. The Reader and Tag now derive session Keys K_{ENC} and K_{MAC} (section 3.1.3).
9. The Reader computes an authentication token:
   T_R= **MAC** (K_M, ($PACEKPu_T$, D'))
   and sends it to the Tag for verification.
10. The Tag computes an authentication token:
    T_T= **MAC** (K_M, ($PACEKPu_R$, D'))
    and sends it to the Reader for verification.

Types of Passwords The specification allows for two types of passwords to be used with electronic passports. These are CAN and MRZ passwords. The Card Access Number (CAN) may be a short static or dynamic password. If the CAN is static, it is simply printed on the passport. If it is dynamic, the Tag randomly selects it and displays it on the passport using low power display technologies such as OLED or ePaper. The MRZ password is a static type symmetric key derived from the MRZ of the electronic passport.

6.2 Terminal Authentication Version 2

In the new specifications (version 2), Terminal Authentication must be performed before Chip Authentication. The purpose of the Terminal Authentication protocol is to allow the Tag to validate the Reader before granting it access to very sensitive biometric information. It works on a two pass challenge-response scheme similar to the one described in 4.1.2. There are several modifications to the Terminal Authentication protocol which is described below.

1. The Reader sends the Tag a certificate chain starting with the local DV certificate and ending with the Inspection System certificate.
2. The Tag verifies the authenticity of these certificates using the CVCA public key.
3. The Tag now extracts the Readers public key ($RPuK$).
4. The Reader generates an ephemeral Diffie-Hellman key pair:
   ($RPrK_{TA}$, $RPuK_{TA}$)
   using the domain parameters (D).
5. The Reader sends the fingerprint of the public key ($Comp(RPuK_{TA})$) and some auxillary data (A_{TA}) to the Tag.
6. The Tag sends a random challenge (R) to the Reader.
7. The Reader using the private key $RPrK$ signs the string
   $(ID_{TA}||R||Comp(RPuK_{TA})||A_{TA})$
   and sends it to the Tag.
8. The Tag verifies the correctness of the signature and the string using the public key ($RPuK$) and other known parameters.

Note: ID_{TA} is a Tag identifier. If BAC is used, its value is the document number printed on the MRZ of the electronic passport. If PACE is used, its value is the fingerprint of the generated ephemeral public key.

6.3 Chip Authentication Version 2

The Chip Authentication protocol in the new specifications is executed only after the Terminal Authentication protocol is executed. This is a necessity since the Chip Authentication protocol requires the ephemeral Diffie-Hellman key pair ($RPrK_{TA}$, $RPuK_{TA}$) which was generated in the Terminal Authentication phase. The Chip Authentication protocol is described below.

1. The Tag sends the Reader its public key ($TPuK$).
2. The Reader sends the ephemeral public key $RPuK_{TA}$ generated during Terminal Authentication to the Tag.

3. The Tag computes the fingerprint of the Readers public key as :
   $Comp(RPuK_{TA})$ using the public key it just received and the auxillary data (A_{TA}). It compares this fingerprint with the one received in the Terminal Authentication stage.
4. The Tag and Reader have enough shared information to derive a seed key (K_{seed}).
5. The Tag generates a random nonce (R). The session keys are computed as $K_{MAC} = \text{SHA-1}(K_{seed}||\text{R}||2)$ and $K_{Enc} = \text{SHA-1}(K_{seed}||\text{R}||1)$.
6. The Tag now computes the authentication token:
   $T_T = \mathbf{MAC}\ (K_{MAC}, (RPuK_{TA}\ ,\text{D}))$.
   The Tag sends R and T_T to the Reader.
7. The Reader uses R to derive the session keys from K_{seed}. It then verifies the authentication token T_T.

7 Noted Vulnerabilities in ePassports

7.1 Common RFID Attacks: Cloning, Eavesdropping, Skimming, and Cross Contamination Attacks

A cloning attack on an ePassport is the attack carried out by an adversary in which a new ePassport containing the same physical and electronic characteristics of a compromised or captured ePassport. A successful cloning attack makes it impossible for a reader to distinguish a cloned from the original ePassport. In first generation ePassports, the active authentication protocol was used to prevent cloning. The security of active authentication is based on the fact that only the original tag has knowledge of the active authentication private key. However, subsequent work demonstrating side channel attacks (power and timing attacks) [30] on ePassport tags showed that it was easy to obtain the active authentication private key from the original tag. Later generation ePassports circumvented this attack by implementing a secondary cloned tag detection algorithm - the chip authentication protocol. The chip authentication protocol restarts secure messaging between the tag and reader once the chip has been authenticated. It is also tied to the reader authentication protocol, which ensures that only valid and certified readers have access to sensitive data on authentic tags. As pointed out by *Blundo et al.*, the chip authentication protocol does not successfully mitigate side channel attacks [31]. An eavesdropping attack on an ePassport is one which permits some adversary to eavesdrop on some legitimate conversation between the victims ePassport tag and a reader, thus possibly giving them the same information that an authenticated and certified reader might obtain. These attacks were fairly easy to carry out early on, since there were to mandatory protocols to deal with these. The use of faraday cages to prevent communication with readers when the ePassport is not in use (preventing skimming), but are useless to prevent eavesdropping attacks. Finally, second and third generation ePassports included terminal (reader) authentication protocols to ensure that only authenticated readers could communicate with tags. In the second generation ePassport protocol, this authentication protocol was used only when access to biometric data was required. This condition was dropped in the third generation specifications.

7.2 Flaws in the First Generation Specifications

BAC and Active Authentication are not mandatory The BAC and Active Authentication schemes are optional in these specifications. If these protocols are not implemented in conjunction with RFID technology, ePassport holders become much more vulnerable to adversaries (*than regular passport holders*). This is because it is easy to skim data from the Tag without the holders knowledge if BAC is disabled and new passports can be built using this data if Active Authentication is disabled. In *regular* passports, there is no Tag that can be skimmed from a distance and therefore cloning the passport requires physical access to the document itself.

Weakness of the BAC Access Keys The BAC is the only protocol designed to protect ePassport holders from skimming and eavesdropping attacks. Unfortunately, the security of the entire protocol is based on the entropy of the two access keys which are derived from data items on the MRZ of the ePassport. While the entropy of these access keys is 56 bits at the maximum, most of these bits are easily guessable. For example, the entropy of the Date of Birth field can be greatly reduced for diplomats and dignitaries (since their date of birth is publically available). Several attacks on Dutch and German ePassport access keys have shown that the entropy of BAC access keys can be reduced to 25-35 bits [32, 20]. It is obvious that this does not provide any real security. Once an adversary gets these keys, they will be able to read and track the Tag throughout the lifetime of the ePassport.

Lack of Access Rules The ICAO first generation ePassport specifications do not have special access rules for secondary biometrics such as fingerprints and iris images which are considered to be more sensitive than other accessible information. This lack of access rules makes it possible for parties to obtain access to information that is very private and they clearly do not require. For example, it is easy for hotel receptionists, car rental agencies, and other organizations where passports are often used for identification, to access and store this sensitive information that they *should* not have.

7.3 Flaws in Second Generation Specifications

Dependence on BAC The EAC specifications still depend on the Basic Access Control protocol to protect the biographic data and headshot of the ePassport holder. The BAC protocol is based on information available on the MRZ of the passport and has an entropy of upto 56 bits. As mentioned in section 3.3.2, the entropy can be greatly reduced through some clever estimations. While access to sensitive biometrics is restricted, biographic information can still be easily obtained by an adversary.

Vulnerability to Attacks by Once Valid Readers ePassport Tags are passive in nature and therefore have no clocks, this means they make estimates of the current date only based on information received from Readers the last time they were activated. This means that it is possible for Readers with expired certificates to read the contents of an ePassport Tag (including sensitive biometrics) if the date on the ePassport Tag was not updated for a long period of time (as would be the case for infrequent travelers).

Vulnerability to Denial of Service Attacks Since the Terminal Authentication protocol is executed only after the Chip Authentication protocol in the EAC operation procedure, it is possible for a malicious Reader to flood the Tag with invalid certificates. Since the Tag has very limited memory, this will cause the Tag to stop functioning as required.

7.4 Flaws in Third Generation Specifications

The third generation ePassport specifications appear to have mitigated all but one of the problems that were present in the earlier generations.

Vulnerability to Attacks by Once Valid Readers ePassport Tags are passive in nature and therefore have no clocks, this means they make estimates of the current date only based on information received from Readers the last time they were active. This means that it is possible for Readers with expired certificates to read the contents of an ePassport Tag (including sensitive biometrics) if the date on the ePassport Tag was not updated for a long period of time (as would be the case for infrequent travelers).

8 Conclusions and Directions for Future Research

The first generation ePassport specifications though still in use in many countries have far too many security risks and its implementation is not advised. The Extended Access Control protocols introduce the concept of mutual authentication between the Tag and the Reader and this helps reduce the risk of skimming attacks. However, a cause for concern is its dependence on basic access control keys which are known to be insecure. While the third generation ePassport specifications address almost every security concern raised by the first and second generation specifications, the expired terminal problem is still a major cause for concern especially for infrequently used ePassports. We described the three generations of ePassport specifications along with their operational procedures and analyzed the flaws of each specification.

References

1. Ismail, N.: RFID: Malaysia's Privacy at the Crossroads? British and Irish Law, Education, and Technology Association. (April 2007)
2. United States Departmment of Homeland Security - United States Customs and Border Protection: Visa Waiver Passport Requirements. (October 2006)
3. Schneier, B.: The ID Chip You Dont Want in Your Passport. The Washnigton Post. (September 2006)
4. Moses, T.: The Evolution of E-Passports: Extended Access Control - Protecting Biometric Data with Extended Access Control. Entrust. (August 2008)
5. Pasupathinathan, V., Pieprzyk, J., Wang, H.: An on-line secure E-passport protocol. In Chen, L., Mu, Y., Susilo, W., eds.: Information Security Practice and Experience, 4th International Conference, ISPEC 2008, Sydney, Australia, April 21-23, 2008, Proceedings. Volume 4991 of Lecture Notes in Computer Science., Springer (2008) 14–28
6. Abid, M., Afifi, H.: Secure e-passport protocol using elliptic curve diffie-hellman key agreement protocol. In: 4th International Conference on Information Assurance and Security. (2008)
7. International Civil Aviation Organization: Doc 9303: Machine Readable Travel Documents - Part 1, Volume 1. (2004)
8. International Civil Aviation Organization: Doc 9303: Machine Readable Travel Documents - Part 1, Volume 2. (2006)
9. Bundesamt fur Sicherheit in der Informationstechnik, Germany: Advanced Security Mechanisms for MRTD's - Extended Access Control v2.1. (2008)
10. Sarma, S., Weis, S., Engels, D.: RFID Systems and Security and Privacy Implications. In Kaliski, B., Kaya ço, c., Paar, C., eds.: Cryptographic Hardware and Embedded Systems – CHES 2002. Volume 2523 of Lecture Notes in Computer Science., Redwood Shores, California, USA, Springer-Verlag (August 2002) 454–469

11. Juels, A.: Rfid security and privacy: a research survey. IEEE Journal on Selected Areas in Communications **24**(2) (2006) 381–394
12. Staake, T., Thiesse, F., Fleisch, E.: Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. In Haddad, H., Liebrock, L., Omicini, A., Wainwright, R., eds.: Symposium on Applied Computing – SAC, Santa Fe, New Mexico, USA, ACM, ACM Press (March 2005) 1607–1612
13. Juels, A.: Strengthening EPC Tags Against Cloning. Manuscript (March 2005)
14. Bailey, D., Juels, A.: Shoehorning Security into the EPC Standard. In De Prisco, R., Yung, M., eds.: International Conference on Security in Communication Networks – SCN 2006. Volume 4116 of Lecture Notes in Computer Science., Maiori, Italy, Springer-Verlag (September 2006) 303–320
15. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: LAMED - A PRNG for EPC Class-1 Generation-2 RFID Specification. In: Computer Standard and Interface. Volume In Press, Corrected Proof., Elsevier Science (2007)
16. Peris-Lopez, P., Tong Lee, L., Li, T.: Providing Stronger Authentication at a Low-Cost to RFID Tags Operating under the EPCglobal Framework. In: IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications – TSP'08, Shanghai, China (December 2008) 159–166
17. Peris-Lopez, P., Li, T., Tong Lee, L., Hernandez-Castro, J.C., Estevez-Tapiador, J.M.: Vulnerability Analysis of a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard. In: Workshop on RFID Security – RFIDSec'08, Budapest, Hungary (July 2008)
18. Nguyen Duc, D., Park, J., Lee, H., Kim, K.: Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. In: Symposium on Cryptography and Information Security, Hiroshima, Japan (January 2006)
19. Koscher, K., Juels, A., Kohno, T., Brajkovic, V.: EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. Manuscript (2008)
20. Juels, A., Molnar, D., Wagner, D.: Security and privacy issues in E-passports. Report, Cryptology ePrint Archive (March 2005)
21. Kc, G., Karger, P.: Security and privacy issues in machine readable travel documents (mrtds). Technical report (2006)
22. Carluccio, D., Lemke-Rust, K., Paar, C., Sadeghi, A.R.: E-passport: The global traceability or how to feel like a ups package. In: WISA. (2006) 391–404
23. Hoepman, J., Hubbers, E., Jacobs, B., Oostdijk, M., Schreur, R.W.: Crossing borders: Security and privacy issues of the european e-passport. Volume 4266 of Lecture Notes in Computer Science., Springer (2006) 152–167
24. Lekkas, D., Gritzalis, D.: E-passports as a means towards the first world-wide public key infrastructure. In Lopez, J., Samarati, P., Ferrer, J.L., eds.: Public Key Infrastructure, 4th European PKI Workshop: Theory and Practice, EuroPKI 2007, Palma de Mallorca, Spain, June 28-30, 2007, Proceedings. Volume 4582 of Lecture Notes in Computer Science., Springer (2007) 34–48
25. Kálmán, G., Noll, J.: On privacy protection in biometric passports. In: ICDS. (2009) 60–64
26. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Transactions on Circuits Syst. Video Techn **14**(1) (2004) 4–20
27. Halfhill, T.: Is RFID Paranoia Rational? (2005)
28. Cerede, G.: Understanding the antenna design challenge. RFIDesign (2006) 10–13
29. InfineonTechnologies: Chip Card and Security ICs SLE 66CLX800PE(M) Family. (2007)
30. Hlavác, M.: Known-plaintext-only attack on rsa-crt with montgomery multiplication. In: CHES. (2009) 128–140
31. Blundo, C., Persiano, G., Sadeghi, A.R., Visconti, I.: Improved security notions and protocols for non-transferable identification. In: ESORICS. (2008) 364–378
32. Avoine, G., Kalach, K., Quisquater, J.: Belgian Biometric Passport Does Not Get a Pass...Your Personal Data Are in Danger! (2007)