The Evolution of Cryptographic Protocols in Electronic Passports

Rishab Nithyanand

University of California - Irvine

Abstract. Electronic Passports are identification documents used primarily for border security. They are capable of storing data, performing low cost computations, and communicating wirelessly. Since 2006, we have witnessed the development of 3 generations of electronic passports and the distribution of over 30,000,000 electronic passports. In this paper, we analyze the cryptographic protocol sets in each of these generations and then go on to present the flaws and security concerns. We also derive a distance-power relationship between the Tag and Reader of an electronic passport.

Key words: Biometrics, ePassports, RFID, Applied Cryptography

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.

Although Malaysia was the first nation to issue electronic passports to its citizens , the first major step towards the global implementation of electronic passports for increased border security was taken by the United States in 2006 when it mandated the adoption of electronic passports by the 27 nations in its Visa Waiver Program (VWP) [1]. The specifications of these ePassports were based on the guidelines issued by the International Civil Aviation Organization (ICAO) in ICAO Document 9303 [2]. However, there were several major security threats that were improperly addressed in ICAO's first generation ePassport specifications [3] [4].

As a result, 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 [5]. The EAC introduced the concept of mutual authentication which allowed the authentication of a Tag and Reader to each other. While these specifications were much more secure than the ICAO's First Generation specifications, there were still some concerns that needed to be addressed [6]. After its release, there were several proposals for the third generation ePassport scheme such as OSEP [7] and an on line authentication mechanism based on the Elliptic Curve Diffie-Hellman key agreement [8]. Finally in October 2008 a new protocol scheme was released by the Bundesamt fr Sicherheit in der Informationstechnik [9]. This is the most recent comprehensive ePassport specification available to date.

1.1 Organization

In section 2, we provide a background of the main electronic passport technologies: Biometrics, RFID, and PKI. We also derive a distance power relationship between the RFID Tag and Reader in ePassports. In section 3, we analyze the cryptographic protocols in the first generation ICAO specifications. In section 4, we analyze the cryptographic protocols used in Extended Access Control (Second Generation). In section 5, we analyze the cryptographic protocols implemented in Extended Access Control with PACE (Third Generation). In section 6, we make our conclusions.

2 ePassport Technologies

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

2.1 Biometrics

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. Commonly used biometrics include head shots, fingerprints, palm-prints, iris images, thermograms, hand geometry, retinal scans, DNA, and voice. Electronic passports favor the use of head shots, fingerprints, and iris images. As discussed by Jain *et al.* in [10], this is determined by parameters such as universality, uniqueness, permanence, performance, collectability, acceptability, and circumvention. The Biometric authentication procedure for electronic passports involves two processes: Registration and Verification.

Unfortunately, without human supervision, it is not always possible to detect the use of prosthetics at the biometric registration or verification stages. As pointed out in [3], biometric spoofing attacks will become easier to implement as automation increases and human supervision of the biometric process decreases.

2.2 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

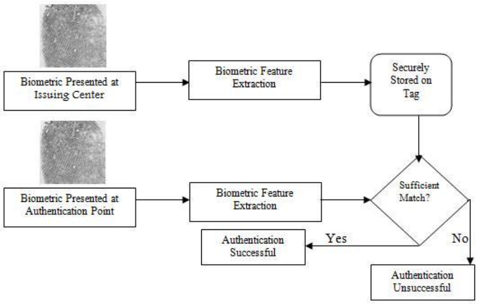
Biometric Presented at Issuing Center
Biometric Feature Extraction
Securely Stored on Tag
Biometric Presented at Authentication Point
Biometric Feature Extraction
Sufficient Match?
Yes
No
Authentication Successful
Authentication Unsuccessful

Fig. 1. Biometric Authentication

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 being used for activities such as behavior profiling and customer tracking [11]. 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.

We will demonstrate how these threats are addressed in each generation of ePassport protocols in the coming sections.

RFID System Components 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.
If we assume the use of an directional antenna on the RFID Reader, then we obtain a relation between distance and received power which is given by the *Friis Transmission Equation* shown below.

$$r = \sqrt{\frac{P_T * G_T * G_R * \lambda^2}{P_R * 16 * \Pi^2}} \tag{1}$$

Where ‘r’ is the distance between the RFID Reader and the RFID Tag, ‘P_T’ is the strength of the transmitted RFID signal whose value is restricted to 1 *Watt* by the Federal Communications Commission (FCC), ‘P_R’ is the strength of the signal received (required) at the Tag, ‘λ’ is the carrier wavelength, ‘G_T’ is the Gain of the transmitting antenna, and ‘G_R’ is the gain of the receiving antenna. Unfortunately, this relation is not suitable for HF RFID systems which are used in ePassports since the wavelength of the carrier is 22.12 meters and therefore building a dipole antenna is not feasible. We will present the working of HF RFID systems in section 2.2.4.

ePassport RFID 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 that we will describe in 2.2.3. As previously mentioned, ePassport RFID systems operate at 13.56MHz (HF) and $\lambda = 22.12$ meters, as a result, designing loop or dipole antennas that can be used on smartcards and ePassports are not possible, instead we use the properties of inductive coupling for signal propagation between RFID Tags and Readers in ePassports. 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 [12].

ePassport Data Elements 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 set of data elements (both mandatory and optional) are shown in Table 1. 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.

Power-Distance relation for ePassport Tags We make use of inductive coupling to transfer power from the Reader to the Tag. For this, we represent the RFID Reader and Tag using the circuit shown in Figure 2. 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

Document Details	Data Group 1
Encoded Headshot	Data Group 2
Encoded Fingerprint	Data Group 3
Encoded Iris	Data Group 4
Displayed Portrait	Data Group 5
Reserved for Future Use	Data Group 6
Signature	Data Group 7
Data Features	Data Group 8-10
Additional Personal Details	Data Group 11
Additional Document Details	Data Group 12
Other Details	Data Group 13
CA Public Key	Data Group 14
AA Public Key	Data Group 15
Persons to Notify	Data Group 16
SOD	-

Table 1. Data Elements to be stored in the LDS

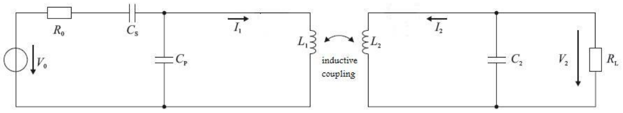

Fig. 2. HF RFID Equivalent Circuit

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 [13].
We first establish the relationship between mutual inductance and distance between the antennas of the Reader and Tag with (2)

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

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.

$$P_{Tag} = (I_1)^2 R_T \tag{3}$$

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

$$R_T = \frac{M^2 R_L}{(L_2)^2} \tag{4}$$

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

$$P_{Tag} = \frac{(I_1)^2 M^2 R_L}{(L_2)^2} \tag{5}$$

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$\propto \frac{1}{x^3}$.

2.3 Public Key Infrastructure (PKI)

The Public Key Infrastructure in ePassports have largely 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 hierarchical structure of the PKI is illustrated in figure 3. 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 (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.

3 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. In this section we provide a description the cryptographic protocols implemented, the operation procedure, and the weaknesses in the ICAO first generation ePassport specifications.

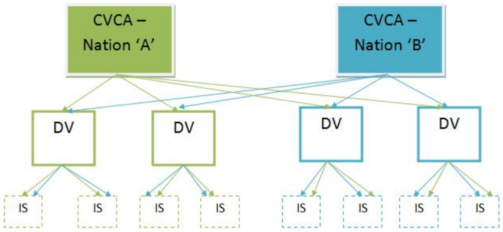

Fig. 3. ePassport Public Key Infrastructure

3.1 Cryptographic Protocols

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.

Passive Authentication The Passive Authentication scheme 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 (either through the PKD or from the ePassport itself), using the public key from the certificate it verifies the digital signature used to sign the data in the groups 1-15 and the SOD. 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.

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. The process is clearly described below.

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}.

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 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.

3.2 Operation Procedure

When a Reader at some Inspection System wishes to read the data on the Tag of a first generation ePassport, the following order of operations must be maintained.
A. Basic Access Control Phase (OPTIONAL)

1. The Inspection System reads the MRZ and computes the Access Keys as described in 3.1.3.
2. If the keys are correctly generated by the Reader, the Tag and the Reader will compute a shared Session Key as described in 3.1.3. These keys will encrypt all future communication.

B. Passive Authentication Phase (MANDATORY)

1. The Reader reads the Security data element (SOD) on the Tag, It then obtains the key KPu_{DV} from the PKD and uses this to verify the validity of the SOD on the Tag.
2. The Reader then reads other data groups from the Tag as needed. Each time a data group is read, it computes the hash and compares the contents with those stored in the element SOD.

C. Active Authentication Phase (OPTIONAL)

1. The Reader compares the MRZ obtained information with the data in data group 1 on the Tag.
2. The Reader reads data group 15 to obtain the Active Authentication Public Key and then invokes the Active Authentication protocol (section 3.1.2).

3.3 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 [14] [4]. 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.

4 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, the operation procedure for second generation ePassports, and some of its flaws.

4.1 Cryptographic Protocols

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.

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.

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.

4.2 Operation Procedure

When a Reader at some Inspection System wishes to read the data on the Tag of a second generation ePassport, the following order of operations must be maintained.

A. Basic Access Control Phase (MANDATORY)

1. The InspectionSystem reads the MRZ and computes the Access Keys as described in 3.1.3.
2. If the keys are correctly generated by the Reader, the Tag and the Reader will compute a shared Session Key (section 3.1.3). These keys will encrypt all future communication.

B. Passive Authentication Phase (MANDATORY)

1. The Reader reads the Security data element (SOD) on the Tag, It then obtains the key KPuDV from the PKD and uses this to verify the validity of the SOD on the Tag.
2. The Reader then reads other data groups from the Tag as needed. Each time a data group is read, it computes the hash and compares the contents with those stored in the element SOD.

C. Chip Authentication Phase (MANDATORY)

1. The Reader runs the Chip Authentication protocol (section 4.1.1).
2. Once the Chip is authenticated, the Reader and Tag establish new session keys and restart secure messaging.

D. Active Authentication Phase (OPTIONAL)

1. The Reader compares the MRZ obtained information with the data in data group 1 on the Tag.
2. The Reader reads data group 15 to obtain the Active Authentication Public Key and then invokes the Active Authentication protocol (section 3.1.2).

E. Terminal Authentication Phase (CONDITIONALLY REQUIRED)

1. If the Reader requires access to Data Groups 3 and 4, the Terminal Authentication protocol (section 4.1.2) is invoked.
2. Access to the sensitive data groups is granted if the Reader has the appropriate access rights.

4.3 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.

5 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 and the operation procedure for third generation ePassports. While this specification is suitable for eSign, eID and ePassport applications, we will describe it only for its relevence to ePassports.

5.1 Cryptographic Protocols

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.

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($\pi||3$).
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.

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 ($ID_{TA}||R||Comp(RPuK_{TA})||A_{TA}$).
8. The Tag verifies the correctness of the message 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.

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 $Comp(RPuK_{TA})$ 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} = SHA-1(K_{seed}||R||2) and K_{Enc} = SHA-1(K_{seed}||R||1).
6. The Tag now computes the authentication token $T_T = \textbf{MAC}\ (K_{MAC}, (RPuK_{TA}$,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.

5.2 Operation Procedure

When a Reader at some Inspection System wishes to read the data on the Tag of a third generation ePassport, the following order of operations must be maintained.
A. PACE Phase (MANDATORY)

1. The User enters either the MRZ key or the CAN as a password.
2. The PACE protocol (section 5.1.1) is executed.
3. Secure Messaging is enabled using the session keys obtained during the PACE execution.

B. Terminal Authentication Phase V2 (MANDATORY)

1. Terminal Authentication protocol (section 5.1.3) is invoked.
2. Access to sensitive data groups is granted by the Tag if the Reader has the appropriate access rights.

C. Passive Authentication Phase (MANDATORY)

1. Before invoking Chip Authentication, Passive Authentication (section 3.1.1) is executed to verify the correctness of the Tags' public key (TPuK).

D. Chip Authentication Phase V2 (MANDATORY)

1. The Chip Authentication protocol (section 5.1.4) is executed.
2. Secure Messaging is restarted using the new session keys obtained on the execution of Chip Authentication version 2.

E. Active Authentication Phase (OPTIONAL)

1. The Reader compares the MRZ obtained information with the data in data group 1 on the Tag.
2. The Reader reads data group 15 to obtain the Active Authentication Public Key and then invokes the Active Authentication protocol (section 3.1.2).

5.3 Flaws in Third Generation Specifications

The third generation ePassport specifications 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).

6 Conclusions

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. Reuters: Us pushes back europes epassport deadline. (2005)
2. ICAO: Doc 9303: Machine readable travel documents - part 1, volume 1. (2004)
3. Juels, A., Molnar, D., Wagner, D.: Security and privacy issues in E-passports. Report, Cryptology ePrint Archive (March 2005)
4. 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
5. ICAO: Doc 9303: Machine Readable Travel Documents - Part 1, Volume 2. (2006)
6. 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
7. 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

8. 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)
9. BSI-Germany: Advanced security mechanisms for mrtd's. (2008)
10. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Transactions on Circuits Syst. Video Techn **14**(1) (2004) 4–20
11. Halfhill, T.: Is rfid paranoia rational. (2005)
12. Cerede, G.: Understanding the antenna design challenge. In: RFIDesign. (2006) 10–13
13. InfineonTechnologies: Chip card and security ics sle 66clx800pe(m) family. (2007)
14. : Belgian biometric passport does not get a pass...your personal data are in danger! (2007)