Keep Out of My Passport: Access Control Mechanisms in E-passports

Ivo Pooters

June 15, 2008

Abstract

Nowadays, over 40 different countries issue biometric passports to increase security on there borders. Among these are the European Union countries. These e-passports are based on the ICAO 9303 standard. One of the goals is including biometric data to increase the security. To prevent fraude on a logical en physical level, security mechanisms are defined in the ICAO standard. In this paper the Basic Access Control (BAC) mechanism is discussed. BAC has been well scrutinized and appears not to be without issues. These issues pose a real threat, but can be mitigated by some adaptions and implementing the extended access control (EAC) mechanism suggested by the ICAO standard.

1 Introduction

The United States initiated the deployment of biometric passports as part of it's US-VISIT program. All 27 nations in the Visa-Waiver Program were mandated to deploy the biometric passport by October 2006. The International Civil Aviation Organization (ICAO) issued guidelines for implementation of the e-passport. This document, 9303 [5], is the defacto standard for e-passports. The ICAO standard specifies face recognition as the main biometrics for identity verification. In addition, the standard specifies fingerprint data and iris data as optional biometrics for verification.

At the time of this writing, over 40 countries are deploying the electronic biometric passport, or e-passport. This new passport stores the personal and biometric data in digital form and contains an RFID chip for communication with passport readers. The goal of the e-passport is strong authentication through documents that unequivocally identify their bearers. This new technology should prevent passport fraude and make identity verification easier and faster.

The e-passport is subject to various security and privacy threats. Among these are *skimming*, *cloning* and *eavesdropping*. The ICAO standard specifies authentication mechanisms for verifying the integrity and authenticity of the data and access control mechanisms to regulate access to the bearers sensitive

data. RFID and biometrics are both privacy-sensitive technologies. Deploying these technologies on a scale of millions of e-passport, requires well-scrutinized access control mechanisms. The standard specifies the optional *Basic Access Control* as the default privacy protection and suggests implementing an *Extended Access Control* for extra protection of biometric data.

Most guidelines provided by the ICAO standard are optional and thus there exist diversity in the e-passport implementations by different countries. This paper shall focus on the access control mechanisms as it is used in the Dutch e-passport. However, the discussions in this paper will apply to most e-passports. In section 2 I start by providing technical background information about the biometric passport. Next, in section 3 security threats and the ICAO countermeasures are described. In section 4 the Basic Access Control is described. The issues concerning this mechanism and access control in general are discussed in section 5. Section 6 discusses some recommendations to mitigate these issues. Finally, this paper is concluded in section 7

2 E-passport Background

2.1 The general e-passport

Figure 1 shows an example of a Dutch e-passport. The layout of the passport may differ for various countries. The RFID chip contains the digital information of the holder. The ICAO defines a Logical Data Structure (LDS) for storing the digital data. Figure 2 shows the layout of this LDS.

In short the LDS contains the following information:

1. Mandatory: the information also physically present on the passport
2. Optional: facial biometric data, fingerprint biometric data and iris biometric data
3. Future: visa information and travel records

In most countries the use of the optionals fields is limited to the facial biometrics. However, as of 28th june 2009 the EU countries must also include fingerprint data in the e-passport [3].

2.2 RFID

The ICAO standard specifies using a Radio Frequency Identification (RFID) module for te e-passport communications. RFID is an upcoming technology for wireless identification of devices. The device RFID chip is usually referred to as RFID tag. RFID tags exist in many forms and applications ranging from identification of products in a logistics context to identification of citizens in the case of e-passports.

Figure 1: An example of a Dutch e-passport

For e-passports the ICAO states that the RFID should conform to the ISO/IEC 14443 [6] standard. These RFID tags operate on 13,56 MHz radio frequency signal. The tags are *passive* which means that they are powered by the RF signal from the reader. The intended read range for the RFID tag according to the ICAO standard is up to 10 centimeters. The requirements for an e-passport RFID device are stricter than for most RFID devices. For example the e-passport requires an RFID device that supports cryptography, has a limited read range and is tamper proof, while a product identifier tag only provides an id and may have a read range of 5 meters.

The ICAO appearantly choose to use RFID technology instead of a smartcard with contact points for the e-passport. The reason for this is not clear from the ICAO standard, but [7] mentions higher data rates, less wear and no change of traditional format as arguments for RFID technology.

2.3 Biometry

Biometry is the process of measuring the biological characteristics. In our everyday life, humans do it all the time. When we meet a friend we perform biometric recognition when checking if his voice sounds as we expect it to sound. Usually, when the term biometric recognition is used, it refers to human-machine interaction instead of human-human interaction. In this paper we also refer to human-machine interaction.

Biometric recognition can be used in two ways: *identification* and *verification*. When a persons biometrics are used to identify him from a database of identities this is referred to as identification. In the case of e-passports, biometrics are (for now) only used for verifying the claimed identity.

Three popular characteristics for biometric verification are *facial data*, *fingerprints* and *iris data*. The process of biometric verification is generally the same for any of the biometrics used. At registration time (e.g. when a citizen requests an e-passport) the person presents a high quality image to the computer which derives a *template* and stores this linked to the identity. At authentication time, the person claims his identity and presents its biometrics. The system

now verifies that the presented biometrics match the stored template.

It is important that a persons biometric data are kept private. An attacker who has aquired the template of fingerprints from his victim, is able to reproduce the original fingerprints with gelatine fingertips. The current state of the art in biometric machines still has a great challenge recognizing fake fingertips.

3 Security Threats and Mechanisms

3.1 Common threats to e-passport security

Because of the privacy-sensitive nature of the e-passport data and the wireless technology used, the ePassport is subject to various security threats. In [7] and [1] the following threats are identified:

Clandestine scanning: ICAO guidelines do not require access control or encryption of RFID communication. This makes the e-passport vulnerable to short-range scanning of the RFID chip, which allows for undesirable leakage of sensitive information, like biometric data.

Clandestine tracking: The RFID protocol, according to [6], emits an ID to avoid collision when communicating. If this ID is unique, this would identification and tracking of a specific e-passport. This ID is sent even if access control is deployed.

Skimming and cloning: When the data of an RFID is leaked, this could allow attackers to clone the RFID chip to a new passport. Authenticating the data on itself is not sufficient to prevent this.

Eavesdropping: After a legitimate passport reader is granted access to the e-passports data, the sensitive data may be leaked by eavesdropping on the communication. A faraday cage in the passports cover would not be sufficient to counter this threat.

3.2 E-passport security mechanisms

The ICAO standard defines the following security mechanisms to ensure privacy and prevent passport fraude:

Passive authentication (mandatory). The goal of passive authentication is to verify the authenticity and integrity of the e-passports LDS. Besides the LDS (section 2.1), the chip also contains a *Document Security Object* (SO_d). The SO_d contains a hash of the LDS data signed by the issuing state.The hash is signed with the *Document Signer* private key. An inspection system will contain or download the Document signer certificate to verify the signature.

Active authentication (optional). The goal is to prevent chip substitution. The e-passport chip may contain an active authentication key pair. The public key is stored in the SO_d, the private key is stored in secure memory. An inspection system would compare the visual MRZ with the MRZ data stored in the LDS to ensure the visual MRZ is authentic. Next, a challenge-response protocol using the active authentication public key will assert that the SO_d is not a copy.

Basic Access Control (optional). The goal is to prevent skimming and eavesdropping. This mechanism is further discussed in section 4.

Extended Access Control (optional). The goal is to provide extra protection for sensitive biometrics. The ICAO standard leaves the design and implementation to the issuing states.

Data encryption (optional). The goal is to further restrict access to the LDS data. The implementation is left to the implementing state.

4 Basic Access Control

4.1 Outline

According to the ICAO standard, the goal of the BAC mechanism is to prevent skimming and eavesdropping. The idea of BAC is that the passport holder should first show his/her consent before any data can be read from the RFID chip. This is accomplished by allowing access only when the access keys are successfully derived from the visual MRZ. This means that a passport holder would have opened and shown his MRZ to the reader and thus provided his consent.

To authenticate the inspection system the following steps are performed:

1. The inspection reads the information from the visual MRZ zone using an OCR-B scanner. Alternatively, this information can be typed in. The most significant 16 bytes of the SHA-1 hash of this information are used to derive a key seed to derive the Basic Access keys (section 4.2).

2. The inspection system and e-passport mutually authenticate and establish a session key. This is discussed in section 4.3.

3. The subsequent communications between the inspection system and e-passport are encrypted and MAC protected. Two key 3DES in CBC mode with zero IV is used for encryption and the MAC is calculated using DES with zero IV.

4.2 Key derivation

For a reader to gain access to the passport chip, it must show its knowledge of the access key pair (K_{ENC},K_{MAC}). The chip itself stores the keys in the LDS. The reader must derive it from the visual MRZ by optical scanning. The following information is read from the MRZ:

1. The document number (usually 9 digits)
2. The date of birth (format YYMMdd in dutch passports)
3. The date of expiry (format YYMMdd in dutch passports)

Even though e-passports may contain more information in the MRZ (dutch passport also include the personal SOFI number), this extra information is not used.

A key seed K_{seed} is derived by taking the most significant 16 bytes of the SHA-1 hash of the MRZ information.

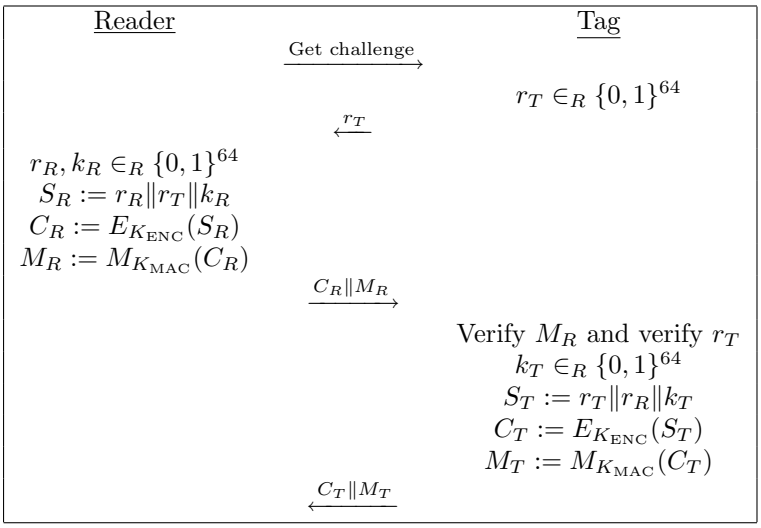
Now, to calculate the two key 3DES K_{ENC}: K_{seed} is concatenated with 1 and hashed using SHA-1 to a 20 byte hash. Bytes 1..8 of the hash form key K_a and bytes 9..16 form key K_b. The parity bits are adjusted to form the definitive two key 3DES key.

To calculate K_{MAC} the same derivation algorithm is used, except that the seed is concatened with 2 instead of 1.

4.3 Mutual authentication and key establishment

Authentication and key establishment is provided by a three pass challenge-response protocol according to ISO/IEC 11770-2 Key Establishment mechanism 6. Two key 3DES in CBC mode with zero IV is used for encryption and the MAC is calculated using DES with zero IV.

The protocol is described by:



Where k_R and k_T are both 16 bytes and r_T and r_R are both 8 bytes. The session keys are then derived by (again) applying the key derivation protocol with $K_{\text{seed}} = k_R \oplus k_T$. These session keys are used to encrypt and MAC any subsequent messages.

5 Access Control Issues

In this section I would like to point out the issues surrounding access control in e-passports. Some issues directly relate to the BAC mechanism as defined by the ICAO, others apply to access control for e-passports in general.

First of all, I believe it was a mistake to make BAC optional instead of mandatory. It was not until august 2007 that the U.S. adopted the BAC in its e-passports as a supplement to the e-passport's signal-blocking covers. A signal-blocking cover alone is not sufficient to protect a citizens privacy. Covers may be left open or accidentaly opened and eavesdropping is still possible.

5.1 Low key entropy

As shown in section 4.2, the access keys are derived from the information on the MRZ of an e-passport. Even though the derived access keys are 16 bytes long, the entropy of the keys is less. Since the only entropy input is that of the MRZ data, the entropy of the derived key is equal to that of the MRZ data. The MRZ data used consists of the document number, date of birth, date of expiry and their respective check digits. For the dutch e-passport, [8] has shown with reasoning and calculations that the entropy of the access key does not come close to the desired 128 bits. Note that other countries may have a little more or less entropy in their document number, but for most cases it will be insufficient.

First, the following is important to note:

1. Only 9 digits on the MRZ are reserved for the document number. Extra digits are ignored for key derivation.

2. The Dutch passport number always starts with the letter 'N' and ends with a checksum number.

3. The Dutch passport numbers are sequential and thus correlated to the expiry date of the passport.

4. Assuming visual of the holder, the year of birth can be reasonably guessed in a range of 10 years.

Now, the entropy can be calculated as follows:

Document Number	7 variable characters (letters + digits)	$(26+10)^7$	36.19 bits
Date of birth	2 digits for year	$365 * 100$	15.16 bits
Date of expiry	validity period of 5 years	$5 * 365$	10.83 bits
Total			62.18 bits

This is a worst-case calculation. If the age of the holder can be guessed in a range of 10 years and the correlation between expiry date and passport number is taken into account, the entropy can be reduced to 35 bits. Brute forcing the access key with 35 bits of entropy takes about 3 hours on a standard computer([8]).

5.2 Tracking

The ISO 14443 RFID protocol makes use of a collision avoidance protocol based on a Unique Identifier (UID). Each RFID chip has such a UID to prevent collisions on the link layer. If this UID is static and different for each e-passport, it gives the oppertunity to identify and thus track e-passports. Since this UID is added to every message, even for a proximity request, higher-level access control mechanisms (like BAC) can not solve this issue.

The collision avoidance protocol does not require this UID to be static. Another possibility is to generate a new random UID each time the tag starts communication with a reader. This is the case with the Dutch e-passport. However, it remains to be researched how random the UID actually is, since it is not easy to have a good PRNG on a low end device like a passive RFID chip.

In [7] it is argued that even if the UID appears random, it creates the possibility for a subliminal channel. Consider the following calculation for the UID:

$$id = E_{k_{\mathrm{NSA}}}(r, passportnumber) \tag{1}$$

If the e-passports are instructed to generate their UIDs like that, the owner of k_{NSA} could decrypt the UIDs and still track the passports. To everybody else the UID would appear just random. This would only be discovered by reverse-engineering the chip.

5.3 Fingerprinting e-passports

A recent skimming threat is described in [4]. This trick allows an attacker to identify the nationality of a passport holder out of 10 different EU nationalities. The attack is possible due to implementation differences at the logical level of the ICAO specification between the various countries.

At the logical level tags and readers communicate using *Application Protocol Data Units*, which are just sequences of bytes in a certain format having certain semantics. E-passport communication is always in a master-slave setup: the reader sends a command APDU and the e-passport replies with a response APDU. The format of these APDU is described in ISO-7816-4 and used in the ICAO standard.

The ICAO standard describes the minimal support for the instructions:

- SELECT FILE (A4)
- READ BINARY (B0)

and the optional instructions (a.o. needed for BAC):

- EXTERNAL AUTHENTICATE (82)
- INTERNAL AUTHENTICATE (88)
- GET CHALLENGE (84)

For the attack two more instructions are used, which are not mentioned by the ICAO standard, but are defined in ISO-7816:

- REHABILITATE (44)
- READ BINARY (B1)

When probing the e-passports of the 10 different nationalities with the above mentioned commands, the responses included the following status words defined in ISO-7816:

- No Error (9000)
- Unknown (6F00)
- CLA Not Supported (6E00)
- Instruction Not Supported (6D00)
- Incorrect P1P2 (6A86)
- Command Not Allowed (6986)
- Conditions Not Satisfied (6985)
- Security Status Not Satisfied (6982)
- Wrong Length (6700)

Except for German and Spanish e-passports, every passport responds differently to one or more of the commands. For the overview of responses given by the different e-passports , the reader is referred to [4]. The attack required just the 7 instructions mentioned and some tweaking of command length in the case of the German and Spanish passport to uniquely fingerprint e-passports from 10 EU nationalities.

This threat is not mitigated by any uniformly adpoted access control mechanism (Basic or Extended), since the attack occurs on the (lower) APDU level.

6 Recommendations

6.1 Signal blocking

As a first line of defense, blocking the RFID signal when transmission is not necessary is a good idea. In the US, the cover of e-passports contains a signal blocking material (faraday cages). This prevents reading any signal from the e-passport while it is closed. Obviously, governments should not rely solely on faraday cages for access control, because there are moments the e-passport will be opened (intentionally or unintentionally) which would leave it unprotected.

However, together with BAC it can seriously hinder tracking and fingerprinting. Tracking would be reduced to moments when the passport is shown to a reader (or somebody else) and then it is just as easy to use the information from the passport extracted by the reader. Fingerprinting for nationality can be useful when it can be conducted automatically on a mass of people, but when it has to be aimed at somebody opening his passport it is probably easier to listen to his language, look at his appaerance or peek in the passport to determine his nationality.

6.2 More key entropy

From section 5.1 it is clear that BAC is vulnerable to eavesdropping attacks on the access key. The low entropy of the MRZ-information is the cause of this. A relatively easy and cheap solution is to increase the entropy of the access key by adding extra information to the MRZ.

As of November 2007, Germany has increased the entropy of its e-passport by replacing its sequential serialnumber document number by a 10-digit pseudo-random alphanumeric document number. For the Dutch e-passport the 9 digit number should be made totally pseudo-random and alphanumeric. This would increase the entropy of the document number alone to over 45 bits giving sufficient entropy. An attacker then has to put at least a lot of effort into cracking the access key.

On the longer run, however, a new authentication scheme is needed.

6.3 APDU response constraints

Section 5.3 showed that too much freedom in interpretation of the APDU protocol creates a skimming vulnerability. The ICAO standard simply is not specific enough about which response APDUs should be replied to which command APDUs. The report does state (p. 21): "A MRTD chip that supports Basic Access Control MUST respond to the unauthenticated read attempts (including selection of (protected) fields in the LDS) with 'Security Status not Satisfied' (6982)".

In [4] the authors propose to view any unexpected APDU commands as unauthenticated read attempts and thus respond to each with 'Security Status not Satisfied'. This would prevent attackers from fingerprinting e-passports based on APDU packets.

It is possible there are other ways of fingerprinting e-passports on a lower level. This is inherent to the ICAO not being specific about certain implementation details. The good news is that a solution does not require extensive research, merely a common interpretation of the ICAO standard.

6.4 Extended Access Control

A special EU committee has drafted an Extended Access Control (EAC) ([3]) mechanism to provide extra protection for biometric data on the e-passport.

Public information on the EAC can be found in [2].

EAC consists of two phases: Chip authentication followed by Terminal authentication. Chip authentication replaces the function of active authentication, namely preventing cloning of e-passport chips. Terminal authentication verifies that the terminal has permission to read the sensitive data on the chip. The access is granted by a chain of certificates that should, in the end, be signed by the e-passport issuing authority.

The EAC still poses some major challenges like creating an international certificate infrastructure and certificate verification for RFID chips like those in e-passports. However, it is an improvement to the BAC mechanism and provides the extra protection that is needed for biometric information.

7 Conclusions

Even though the e-passport is allready widely deployed and in use, there still remain security issues to be resolved. From section 5 is appears that BAC does not completely counter the threats mentioned in section 4. Clandestine scanning, although limited, is still possible by using lower level APDU probing. Eavesdropping attacks are feasible, since the entropy of the access keys is low enough for off-line guessing.

We discussed some recommendations for improving the security to a minimum level. Signal-blocking material would greatly reduce the threat of tracking and fingerprinting or other clandesting scanning. Furthermore, a more explicit guideline on dealing with unexpected command APDUs and other low level protocol commands will reduce differences between implementations per country.

Finally, the EU committee is paving the way to a more secure solution for biometric data on the e-passport chip. The EAC mechanism should solve some of the mentioned issues by actually authenticating genuine readers.

References

[1] D. Molnar A. Juels and D. Wagner. Security and privacy issues in e-passports, 2006.

[2] BSI. Advanced security mechanisms for machine readable travel documents - extended access control (eac). technical report tr-03110, bsi, bonn, germany. Technical report, BSI, 2006.

[3] EU Commission. New, secure biometric passports in the eu, strenthen security and data protection and facilitates travelling. EU Website rapid press release, June 2006.

[4] E. Poll H. Richter, W. Mostowski. Fingerprinting passports, 2007.

[5] ICAO. *Document 9303, machine readable travel documents*, October 2004.

[6] ISO/IEC. *ISO 14443 - Identification Cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1 to Part 4*, February 2007.

[7] B. Jacobs et al. J. Hoepman, E. Hubbers. Crossing borders: Security and privacy issues of the european e-passport. IWSEC 2006, 2006.

[8] H. Robroch. epassport privacy attack. presentation, Riscure, July 2005.

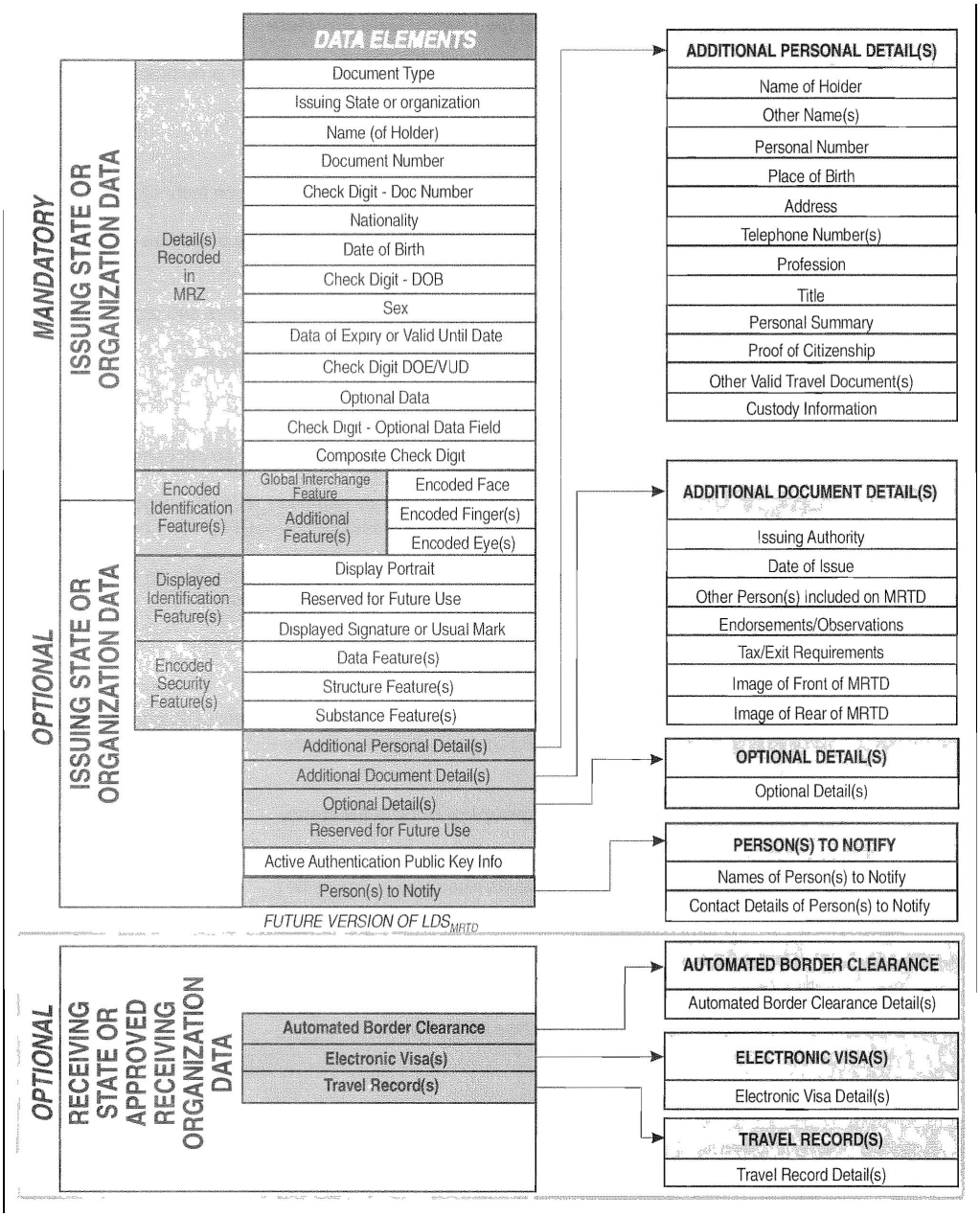


Figure 2: The LDS for e-passport data. The figure shows which data elements are mandatory, optional or for future use.