Term Paper

II3230 Information Security

Security of Biometric Passports: How Countries Trust and Distrust Each Other

Muhammad Aditya Hilmy / 18217025

Information Systems and Technology Study Program
School of Electrical Engineering and Informatics
Institut Teknologi Bandung

2020

Abstract

As the primary means of identification for travelers, passport is a very important document where security is one of the highest concerns. Therefore, it is paramount for countries to take measures in making sure that passports can be highly trusted. One of the efforts of making passports more trustable is by introducing biometric passports. In alignment with its name, a biometric passport stores the biometric information of its bearer. Although a biometric passport looks no different than a regular passport, the infrastructure and technology needed to enable biometric passports is much more complex. This paper will discuss the technology and infrastructure behind biometric passports, also known as the electronic Machine Readable Travel Document (eMRTD).

Keywords: eMRTD, biometric passport, PKI, certificate, digital signature, ICAO

Chapter 1. Introduction

Civilization is now in the era of globalization, when mankind is more connected than ever. People cross international borders in record volumes. According to Our World in Data, in 2018, the number of international travels reached 1.4 billion [1]. The growing number of international visitors also means that countries need to work harder to prevent malicious people from entering their border while making sure well-intentioned people are able to enter their borders with minimal effort. One of the measures countries take to do that is by making sure that all passports screened at the port of entries are legitimate; that is, not counterfeit and used by the person stated in the passport.

Conventional non-biometric passports have some security measures comparable to banknotes. They could have specialized paper, UV-visible ink, microprints, and so on. Unfortunately, as counterfeiters get more sophisticated and technologies get cheaper, those measures can be rendered useless.

Biometric passports leverage sophisticated technologies, such as biometric matching, Radio Frequency Identification (RFID) and Public Key Cryptography, to enable countries to check the legitimacy of passports entering and exiting their borders [2] with greater confidence than traditional physical measures. In this paper, the author will discuss the technology behind biometric passports and how they work together.

Chapter 2. Discussion

2.1. Biometric Authentication in eMRTD

There are several steps in biometric authentication, namely *identification*, *capture*, *extraction*, *template creation*, and *matching* [3]. *Identification* means making sure that the identity of the subject is known. *Capture* means scanning the image of the subject's biological features such as face, iris, or fingerprint. *Extraction* is the process of turning the captured image into an intermediate form, such as fingerprint minutiae. *Template creation* is the process of creating biometric templates from an intermediate form. Finally, *matching* is the process of comparing two biometric templates to see whether the stored template matches the biometric feature it is verified against.

According to ICAO Doc 9303 Part 9 [3], the ICAO recognizes three types of biometric authentication: facial recognition, fingerprint recognition, and iris recognition. Facial recognition is the only method required by the standard, and the implementation must be in compliance with ISO/IEC 19794-5 specifications. Fingerprint and iris recognition are optional, and they must comply with ISO/IEC 19794-4 and ISO/IEC 19794-6 respectively.

The implementation of how a biometric image is transformed into a template differs according to vendors [3]. For that reason, the International Civil Aviation Organization (ICAO) requires biometric passports to store the biometric information in a form that can be extracted into a template regardless of the biometric device manufacturer countries used. The biometric information can be stored in the form of an image which can be compressed using the JPEG or JPEG 2000 compression schemes. Additionally, countries are allowed to also store the biometric template in the passport chip for use in systems under the control of the issuing country.

2.2. Proximity Integrated Circuit Card (PICC)

PICC is a component which has an integrated circuit chip and a coil of wire, embedded inside a plastic wafer [4]. It is able to communicate with a reader called Proximity Coupling Device (PCD) without having to have a physical contact. It works by taking advantage of magnetic induction in the coil to power the chip, and radio frequency to exchange data between PICC and

PCD. There are several standards for PICC, but the one used in biometric passports worldwide is the ISO/IEC 14443 standard [2], which uses radio frequency 13.56 MHz.

Unlike a magnetic stripe card, PICC communicates with the reader instead of being read. It makes PICC much more secure. PICC is able to authenticate the reader, which means only authorized readers are able to read and write the contents of the card. This is necessary since a biometric passport contains sensitive information such as birth date and biometric images.

PICC and PCD communicate in Application Protocol Data Unit (APDU), which is simply sequences of bytes arranged in a certain way. APDUs are standardized in the ISO/IEC 7816 specification. There are two kinds of APDU, command and response. Command APDU is sent by PCD to PICC, while response APDU is sent by PICC to PCD as a response to the command APDU. Figure 2.2.1 shows the structure of each APDUs.

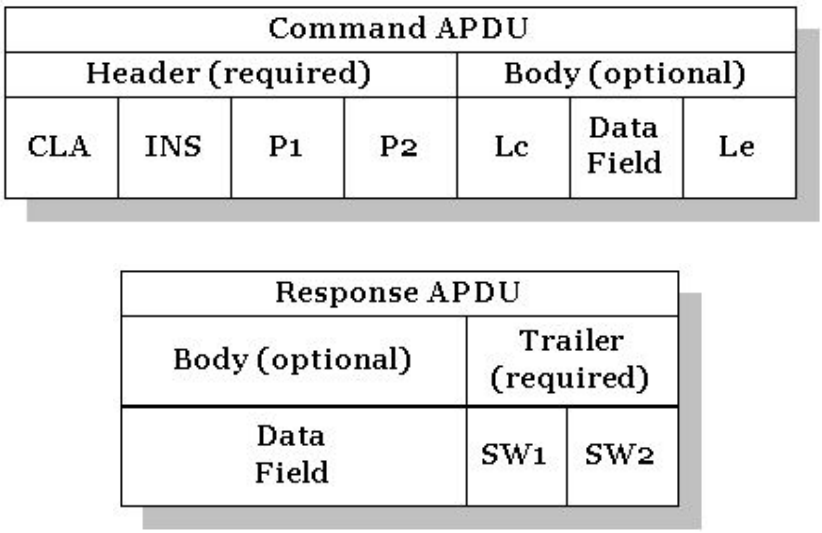

Figure 2.2.1. APDU structure (source: oracle.com)

2.3. Public Key Infrastructure (PKI)

One of the primary technologies that enables eMRTDs is the Public Key Infrastructure. In hindsight, Public Key Infrastructure is the one technology that enables countries to decide whether to trust the passport or not. It also allows eMRTDs and reader machines to exchange messages securely.

2.3.1. Public Key Cryptography

To understand PKI, one needs to understand what Public Key Cryptography is. Simply put, Public Key Cryptography is a method of cryptography in which two keys-namely private key and public key-are involved [5]. There are two use cases that are relevant in the discussion: asymmetric encryption and digital signature.

In asymmetric encryption, the goal is to conceal the message exchanged between two parties so that the message can only be read by the intended recipient. Firstly, the sender uses the recipient's public key to encrypt the message to make a *ciphertext*. Secondly, the ciphertext is sent to the recipient through unsecured communication medium. Finally, the recipient uses its own private key to decrypt the message [5].

In digital signature, the goal is to verify the authenticity of a message; to ensure that the message being received is indeed written by the actual sender. Firstly, the sender creates a *digital signature* of the message using its private key. Secondly, the message along with the digital signature is sent to the recipient through an unsecured medium. Finally, the recipient validates the message using the plaintext message, its digital signature, and the sender's public key. If after a series of mathematical calculations those three data matches, the recipient can be sure that the message is sent by the sender untampered [6].

2.3.2. Digital Certificate

Public key cryptography provides a way to conceal and validate messages. Unfortunately, it shifts the vulnerability to the process of obtaining the public key. The challenge of public key cryptography is to make sure that the public key being received is untampered and authentic. To address the problem, a *digital certificate* can be used.

The purpose of a digital certificate, same as a typical certificate, is to provide a proof of something. In this case, it provides a proof of public key ownership, identity, or privileges. The certificate is issued by a Certification Authority (CA) [7]. A Certification Authority also has its own certificate, which is issued by another CA and so on. A

Certification Authority without any issuing CA is known as a Root Certification Authority [8].

Analogous to a typical certificate where the credibility of the certificate depends on the credibility of the issuer, a digital certificate is *trusted* if the certificate issuer (i.e. the CA) is also trusted [8]. A Certification Authority can be trusted if its certificate is issued by another trusted CA. A Root CA, however, must be explicitly trusted. This is known as a *chain of trust*. Figure 2.3.2.1 shows an illustration of a chain of trust.

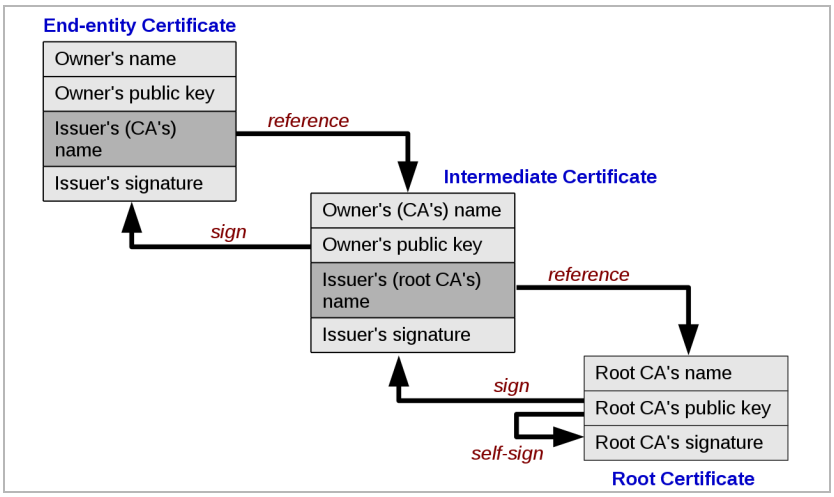

Figure 2.3.2.1. Chain of trust (source: commons.wikimedia.org)

There are several standards on how a digital certificate is implemented. The one in which PKI in biometric passports is based on is X.509 [9]. An X.509 certificate contains the following information [10]:

1) To-Be-Signed Certificate
    a) Version
    b) Serial number
    c) Signature
    d) Issuer
    e) Validity
        i) Not before
        ii) Not after
    f) Subject

g) Subject public key
    i) Algorithm
    ii) Public key
h) Issuer unique ID
i) Subject unique ID
j) Extensions
    i) Extension ID
    ii) Is extension critical
    iii) Extension value

2) Signature algorithm
3) Signature value

For Subject and Issuer fields, a standard set of attributes is defined in X.520 specification. It includes:

1) Country
2) Organization
3) Organizational unit
4) Distinguished name
5) State or province name
6) Common name
7) Serial number

2.3.3. Public Key Infrastructure in MRTDs

In general, Public Key Infrastructure includes all entities involved in the creation, and management of digital certificates to facilitate the use of public key cryptography [8]. According to ICAO Doc 9303 Part 12 [9], the PKI schema used in eMRTDs is simpler than internet PKI. Some of the notable differences include:

1. There is no intermediate Certification Authority; only one Country Signing Certification Authority (CSCA) per country.
2. Signature verification must be guaranteed to work 5-10 years after issuance.

PKI scheme in eMRTD has the following roles:

1) Country Signing Certification Authority (CSCA)

   CSCA is where the trust chain of the eMRTDs begins. The keys of CSCA are used to derive Document Signer certificates, as well as some other certificates. Due to the fact that CSCA sits on top of the trust chain and is relatively static, the CSCA certificate must be self-signed and kept very securely.

2) Document Signers

   Document Signer certificate is issued by the CSCA, and is used to sign the information contained in the eMRTD, specifically the Document Security Object. The private key of a Document Signer is kept private by the issuing country, and the public key is stored as a Document Signer certificate in the eMRTD.

3) Inspection Systems

   Inspection Systems are the ones that read the information contained in eMRTDs. Inspection Systems have the responsibility to perform checks and authentications to make sure the eMRTD is legitimate and the information contained in it is authentic and untampered.

4) Master List Signers

   Master List Signers are the ones signing a list of CSCA's certificates for the purpose of bilateral exchange of certificates.

5) Deviation List Signers

   Deviation List Signers are the ones signing a list of Deviations, i.e. a list of MRTD practices that differs from the standards outlined in ICAO Doc 9303.

Sometimes, a certificate needs to be revoked before its expiry date. This could happen when the key corresponding to the certificate is compromised. To address the issue, ICAO requires all CSCA to issue a Certificate Revocation List (CRL) at least once every 90 days, even when there is no certificate being revoked.

Figure 2.3.3.1 illustrates the PKI chain of trust of the eMRTD system.

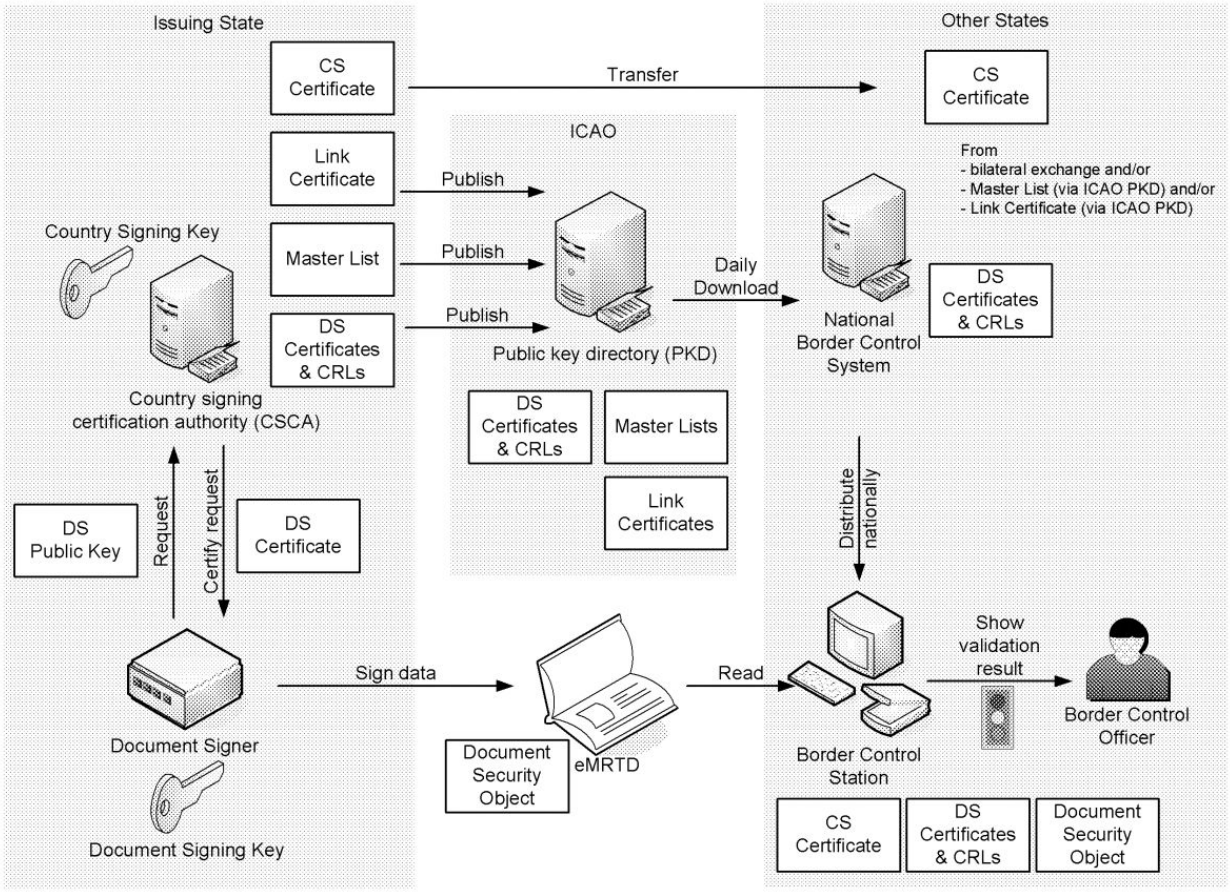

Figure 2.3.3.1. eMRTD chain of trust (source: icao.int [11])

2.4. Security of Electronic Machine Readable Travel Document (eMRTD)

Unlike credit cards or national ID cards where normally the issuing authority of the cards also control the reader devices, eMRTDs should be electronically readable by inspection systems of various countries with different implementations. As a result, eMRTDs must employ various techniques that ensure compatibility while maintaining a high level of security. To achieve this, eMRTD uses several steps of procedures to be followed before allowing inspection systems to retrieve the information contained in the chip. Additionally, eMRTD also provided several methods to allow inspection systems to ensure the authenticity of the document.

2.4.1. Preventing Unauthorized Access

Since eMRTD uses radio frequency to exchange messages, it has a risk of being skimmed or eavesdropped. As a consequence, the eMRTD chip must only allow communication when the document is being properly read. To address this issue, eMRTD provides two methods of authentication: Basic Access Control (BAC) and Password Authenticated Connection Establishment (PACE). In a nutshell, those two methods use information in the Machine Readable Zone (MRZ) of the MRTD that is visually present to derive a cryptographic key. This way, an inspection system should have a visual on the MRTD before being able to read the data using radio frequency. In the case of biometric passports, it means that the passport must be placed on the reader, opened. Aside from that, issuing countries can add a protective foil in the passport cover to block radio frequency when the passport is closed.

Figure 2.4.1.1. Machine Readable Zone (source: www.nicomsoft.com)

2.4.2. Preventing Transmission Eavesdropping

Some of the data transmitted between the eMRTD and reader device, such as birth date and biometric data, are sensitive. To prevent unintended parties from eavesdropping the transmission, a way of securely exchanging messages is necessary.

To allow for secure messaging, both the eMRTD and the reader device must agree on a shared secret key. Moreover, the shared key must not be static to prevent replay attacks. To achieve this, both devices derive a session key from the BAC or PACE process, without ever transmitting the shared key. Additionally, both devices need to agree on which encryption algorithm to use. Once a key and algorithm are agreed, the eMRTD and inspection system exchange encrypted messages. The secret key is dismissed when the inspection system and eMRTD disconnect.

2.4.3. Ensuring the Authenticity of the eMRTD

Previous security measures guard against unauthorized access and eavesdropping. They, however, do not check whether the eMRTD is actually issued by the issuing country. To do this, a security measure called Passive Authentication (PA) is used.

Passive Authentication looks at an information stored in the eMRTD known as the Document Security Object (DSO). Some of the data included in the DSO are: Document Signer certificate, hash of the eMRTD data groups, and the signature of the hash signed by the Document Signer. Using the DSO, the inspection system is able to:

a) Verify the integrity of the data groups stored in the eMRTD by calculating the hash of the data groups and comparing it with the hash stored in the DSO.
b) Verify the integrity of the hash by checking the digital signature using the public key in the Document Signer certificate.
c) See whether the eMRTD is authentic by looking at the chain of trust of the DS certificate to the CSCA certificate explicitly trusted by the inspection system.

2.4.4. Preventing Chip Duplication

Previous security measures do not guard against *chip duplication*, since there is no data that is not retrievable from the chip. Theoretically, a malicious party can read all the data in the eMRTD and copy it into a new chip. To prevent this, there must be some kind of measure to know if the chip is not genuine. To address this issue, eMRTD employs a security measure known as Active Authentication.

Active Authentication uses an asymmetric key pair. The private key is known only to the chip and is stored securely. The public key is stored and accessible to the inspection system. When performing Active Authentication, the inspection system sends a challenge nonce to the chip, in which the chip replies with a signature signed using the Active Authentication private key. The inspection system will then verify the signature using the Active Authentication public key retrieved from the chip.

The inspection system is able to trust the Active Authentication public key since the public key is also signed by the Document Signer and can be verified using Passive Authentication.

2.5. Distribution of the Country Signing Certification Authority (CSCA) Certificate

As discussed in previous sections, the topmost element of the chain of trust is the CSCA certificates. CSCA certificates must be explicitly trusted by countries, thus there must be a way of securely distributing these CSCA certificates. In general, there are two ways of distributing the CSCA certificate: through bilateral agreement between countries, and by participating in the ICAO Public Key Directory (PKD).

2.5.1. Bilateral Agreement

ICAO Doc 9303 outlines several ways of securely exchanging the certificates through bilateral agreement [9]. They include:

1. Using diplomatic couriers/pouches.
2. Exchanging files through email.
3. Downloading files from a website of the issuing CSCA.
4. Downloading files from an LDAP server of the issuing CSCA.

The list above is not exhaustive. How the certificates are technically exchanged depends on the agreement between the countries.

2.5.2. ICAO Public Key Directory (PKD)

ICAO provides a service known as ICAO PKD to facilitate certificate exchange between participating countries. The PKD infrastructure is equipped with redundancies to minimize a single point of failure [11]. Firstly, there are two redundant sites located in Germany and the United Arab Emirates. The sites are designed to substitute one another in the case of failure. Secondly, there are also redundancies within the two sites. Load balancers and redundant networks are used. Moreover, for added security, a Hardware Security Module (HSM) is used in both sites to keep the cryptographic keys secure.

ICAO PKD serves certificates using Lightweight Directory Access Protocol (LDAP) server. Participating countries are given an Access Certificate and a writable subtree in the LDAP directory to upload their certificates. Once a participating country uploads a certificate, the certificate will be reviewed for compliance. Initially, the uploaded certificate is reviewed automatically. When the automatic test fails, however, the certificate in question will be reviewed by an operator. After a certificate is accepted, it enters a "cool-down period." During that period, the certificate is withheld for publication for a certain amount of time. This is done to prevent false upload or false acceptance. Also during that period, accepted certificates can be revoked [11].

In addition to countries certificates, the PKD LDAP server also contains several additional information regarding the certificates. It includes the registry information and the Certificate Revocation List (CRL).

Uploaded certificates are publicly accessible from the ICAO PKD website. Everyone can access the certificate anonymously from the ICAO PKD website in the form of an LDIF file. Participating countries can also download the certificates and their additional information from the LDAP server. Due to the rigorous process of maintaining the public key certificates, participating countries are able to explicitly trust the certificates listed in the ICAO PKD.

Chapter 3. Conclusion

There are plenty of security measures countries take to be able to decide whether to trust a passport or not. To make sure the measures work anywhere in the world, countries collaborate to create a standard, which is maintained by the International Civil Aviation Organization (ICAO).

Briefly speaking, the biometric passport system utilizes various technologies including biometric matching, proximity integrated circuit, public key cryptography, and public key infrastructure. Biometric matching ensures that the person handing the document is actually the bearer of the document. Proximity IC stores the document bearer's information and protects the information on the passport from skimming. PKI of the eMRTD system ensures that countries can establish a chain of trust to authenticate the document. Additionally, ICAO maintains the Public Key Directory service, which facilitates countries in exchanging their public key certificates without having to establish bilateral agreement between all ICAO member states.

The sophisticated security measures employed by biometric passports provide a systematic way of verifying the authenticity of passports, in addition to physical security measures of traditional non-biometric passports. Cryptographic means of securing the passport are mathematically guaranteed to be harder to counterfeit. Nevertheless, as technology progresses, it is inevitable that these security measures will become obsolete.

References

[1] M. Roser (2020) - "Tourism". Published online at OurWorldInData.org. Retrieved from: 'https://ourworldindata.org/tourism' [Online Resource]

[2] A. Atanasiu and M. I. Mihailescu, "Biometric passports (ePassports)," *2010 8th International Conference on Communications*, Bucharest, 2010, pp. 443-446.

[3] International Civil Aviation Organization. "Doc 9303, Machine Readable Travel Documents, Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs." Internet: https://www.icao.int/publications/Documents/9303_p9_cons_en.pdf, [Apr. 18, 2020].

[4] *Identification cards – Contactless integrated circuit(s) cards – Proximity cards*, ISO/IEC 14443:2018, 2018

[5] N. Li (2009) Asymmetric Encryption. In: LIU L., ÖZSU M.T. (eds) Encyclopedia of Database Systems. Springer, Boston, MA

[6] B. Carminati (2009) Digital Signatures. In: LIU L., ÖZSU M.T. (eds) Encyclopedia of Database Systems. Springer, Boston, MA

[7] C. Adams (2011) Certificate. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA

[8] J. Huang and D. Nicol, "An anatomy of trust in public key infrastructure," *International Journal of Critical Infrastructures*, 2017, pp. 238.

[9] International Civil Aviation Organization. "Doc 9303, Machine Readable Travel Documents, Part 12: Public Key Infrastructure for MRTDs." Internet: https://www.icao.int/publications/Documents/9303_p12_cons_en.pdf, [Apr. 22, 2020].

[10] D. Cooper, et al. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." Internet: https://tools.ietf.org/html/rfc5280, [Apr. 22, 2020].

[11] International Civil Aviation Organization. "Machine Readable Travel Documents Guidance Document: PKI for Machine Readable Travel Documents." Internet: https://www.icao.int/Security/FAL/PKD/Documents/PKDTechnicalDocuments/GuidanceDocument-PKIforMachineReadableTravelDocuments.pdf, [Apr. 24, 2020].