RFID chips and EU e-passports: the end of privacy?

By Nikita Maria, PhD Candidate, Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece, nikita_ma@yahoo.gr

Abstract

Radio Frequency Identification (RFID) technology is in wide deployment and has been used to many applications for decades. The principal advantage of this technology is that it automatically identifies objects using electromagnetic waves to communicate with a reader without requiring contact and line of sight.

As the technology evolved and offered large memory capacity it was used as a storage medium for electronic passports (e-passports). The e-passport is the digital version of the paper passport and its goal is to provide stronger identity authentication than the classic one. It was believed that it was able to ease identity checks, lessen the amount of human errors, protect against manipulation of travel documents and improve border security. But the fact that biometric data can be stored to the e-passport; privacy and security risks are posed for the holders. So, this new passport turned out to be much more intrusive than the traditional one.

RFID chips used in e-passports are equipped with protection mechanisms but they still have lots of technical flaws and they are vulnerable to skimming and eavesdropping. The main problem stems from the fact that the data contained on the e-passport are transferred wirelessly, so it is vulnerable to anyone having the necessary equipment.

This paper focuses on the use of RFID technology in EU e-passports. Particularly a short description of the technology and its advantages are given and even more attention is given to the threats that are posed to the holder's privacy. Finally, data protection issues and the proposed EU Regulation are presented.

1. Introduction

Radio Frequency Identification (RFID) is a technology that uses wireless communication for identification purposes. It is not a new technology since it dates back in 1948 when it was first used for military applications. From then it has been used in many different applications such as transportation, supply chain and product management, mobile asset management, retail management and security applications. The key characteristic that differentiates one RFID application from another is the purpose of identification.

The RFID technology was also chosen to be used as a storage medium for e-passports. Since the old paper based passports were suffering from forgery and fraud, e-passports, the digital version of the paper passport, were introduced to reduce fraud and support immigration processes. Moreover, the International Civil Aviation Organization (ICAO) published the standards and specifications for these electronically enabled passports with biometric identification capability.

Undoubtedly, RFID offers powerful benefits. However, like most technological applications, its use has raised important privacy issues. Particularly, when information provided by these smart objects in a wireless way is associated with personal data, as in the case of e-passports, many security and privacy concerns arise.

This paper examines the use of the RFID technology in e-passports. Moreover, in the next chapter the contribution of the International Civil Aviation Organization is

mentioned. In the 3rd chapter the e-passport's characteristics and the technologies used to strengthen national border security, protect against e-passport manipulation and reduce identity theft are discussed. In chapter 4 the evolution of the e-passport through time is presented. The three generations of the e-passport and the suggested each time communication protocols and security mechanisms are examined. In chapter 5 the e-passport's flaws and vulnerabilities are described and finally in chapter 6 the ICAO's recommended standards and the EU Council's Regulation are presented.

2. The International Civil Aviation Organization

While the number of people travelling was growing, the need for more efficient and secure checks increased. This led to the introduction of Machine Readable Travel Documents which involved during time.

The International Civil Aviation Organization (ICAO) is a specialized agency that has the mandate and responsibility of establishing, maintaining and promoting standards. It recommends practices related to the issuance and verification of Machine Readable Travel Documents, and related border control issues. ICAO issues passport standards as recommendations to the national governments and its' aim is to succeed universal infrastructure and interoperability of travel documents.

ICAO's work on machine-readable travel documents began in 1968 with the establishment of the ICAO Panel on Passport Cards and in 1980 published for the first time the Doc 9303 as "A Passport with Machine Readable Capability" and served as the guideline for issuing machine-readable passports.

3. EU e-passport technologies

E-passports are Machine Readable Travel Documents that contain a contactless integrated circuit in which data is stored concerning the holder. E-passports' aim is to strengthen national border security, protect against manipulation of travel documents and reduce identity theft.

The layout of the passport may differ for various countries. However, all e-passport's have a symbol that is international and signifies that the passport contains a contactless microchip with data storage of at least 32kB on which data about the passport holder is stored. The symbol (Figure 1) should appear on the front cover of the passport near the top or the bottom [Doc 9303, Part 1, Vol. 2].

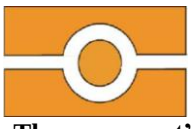

Figure 1: The e-passport's symbol

In 2006, ICAO published the specifications for electronically enabled passports with biometric identification capability. A Logical Data Structure (LDS) for storing the data on the chip was defined. In particular it defined that the information which are already shown on the paper passports are mandatory and facial biometric data (a high quality digital image with JPEG 2000 format), fingerprints and iris are optional.

The format standards for facial data, when used, include the whole head centered with the hair not covering the face and the eyes open on the same horizontal line. The neck

and the shoulders of the e-passport holder must also be included in a single background color without shadows.

The data stored on the chip should be identical to the printed information on the paper passport. This is necessary for two reasons, in case the chip fails the e-passport is still a valid travel document and the holder can use it and also at any time he is aware which data is stored on the chip of his passport without the need of any technical equipment. The second reason is not valid in case the e-passport includes in its chip biometrical data, such as fingerprints, he needs suitable technical equipment to have access.

In 2011, ICAO proposed the option to include electronic travel history, visas and automated border clearance applications in the e-passports [ICAO Working Paper, 2011].

3.1 Biometric data

Biometrics refers to measurable biological or behavioral aspects of a person and can be used for automated recognition [NSTC, 2006]. They are powerful identifiers and the most irrefutable proof of a person's identification that promotes security and efficiency in access controls since they are unique and it is not possible to be shared or duplicated [Vakalis I., 2011].

According to Cavoukian A. (1999) biometrics can be used in two ways: for identification and authentication/verification. In the case of identification, a computer system compares a person's biometric characteristic, e.g. fingerprint, with all biometric samples stored in its database. If it matches with one of them then the person is identified. This is called one-to-many match.

In the case of authentication, the person presents a live biometric and it is compared with the one to a stored sample that is given previously. If they match the authentication is completed and this is called one-to-one match. In the latter case the biometrics are not stored in a central database, a template of each person's biometrics could be stored on a smart card that the person possess and is responsible for.

However, the information that biometrics provide is sensitive and this strong match between a person's biometrics and his physical existence poses serious privacy risks. In the case of e-passports, biometric data is used for authentication and is stored on a RFID chip that is embedded in the paper passport.

3.2 R.F.I.D. technology

The selection of the right technology to store the holder's data to conduct border control in a cohesive manner was a big challenge. According to Article 1 par. 2 of Regulation (EC) No 2252/2004 e-passports shall include a storage medium with sufficient capacity and capability to guarantee the integrity, the authenticity and confidentiality of the data stored. This medium should additionally prevent unauthorized access; include enhanced anti-forgery, counterfeiting and falsification standards and standards for the quality of the data stored.

The minimum standards and features determined by ICAO are the features of usability, data capacity and performance so as to achieve high speed, high capacity and high security solution. Specifically, the only technology that doesn't require line-of-sight in order to achieve contactless mode of operation to facilitate the job of border authorities is contactless IC chips. Also, the minimum data storage capacity

needed for biometric verification given the inclusion of facial images and fingerprints is approximately 15-20kB and the only technologies with sufficient capacity are contact IC chips, contactless IC chips and optical memory. Finally, the technology that succeeds shorter transmission times is contactless IC chips.

Overall, the only technology that meets all three considerations of usability, data capacity and performance is the contactless IC chip [ICAO Technical Report, 2004]. The RFID technology uses contactless IC chips, thus it was chosen to be used as a storage medium for e-passports.

An RFID system consists of the RFID tag and the reader. The tag is attached to the object, in our case the passport, and communicates wirelessly with the passport reader using an antenna. RFID technology offers powerful benefits to its adopters and today is already being used in a variety of applications such as payment systems, access control, supply chain activities and animal and human tracking [Nikita M., 2011].

While RFID has existed for decades, its use has raised important risks. Particularly, because the information provided in a wireless way is associated with personal data, many security and privacy concerns arise. In the case of e-passports, it was believed that it was able to ease identity control, lessen the amount of human errors, protect against manipulation of travel documents and improve border security. But the fact that biometric data can be stored to the e-passport; privacy and security risks are also posed to the holders.

Although RFID chips used in e-passports are equipped with protection mechanisms, they still have lots of technical flaws and they are vulnerable to skimming and eavesdropping. The main problem stems from the fact that the data contained on the e-passport is transferred wirelessly, so it is vulnerable to anyone having the necessary equipment.

4. E- passport generations

The first generation of e-passports appeared in November 2004 when ICAO published the Doc 9303 in which recommended a set of guidelines and standards for e-passports. According to Doc 9303, e-passports should use an RFID chip embedded in the passport cover in which holder's personal data and biometric data is stored. In this generation, according to ICAO the three communication protocols that should be used by e-passports as security mechanisms are Passive Authentication, Basic Access Control, and Active Authentication.

The Passive Authentication (PA) protocol is mandatory to be used to prove the integrity and the authenticity of the data stored. A cryptographic computation is used by the reader to verify the authenticity using the public key of the issuing country. Although the authenticity of the data can be verified, PA cannot detect cloning and doesn't prevent unauthorized access.

Active Authentication (AA) was proposed by ICAO as an optional protocol to prevent the cloning problem. In this case, to verify the authenticity of the chip, the chip must prove to the reader that it possesses a private key. Then the reader verifies its correctness using the public key, signed by the issuing country and verified by the PA protocol. AA adds complexity, requires the chip to have processing capabilities and doesn't prevent skimming and eavesdropping.

Basic Access Control (BAC) is also an optional protocol recommended by ICAO to prevent skimming and eavesdropping. It causes the RFID chip to check the access to

its data and allow only authorized readers to gain access. A chip is protected by the BAC mechanism and the reader's authenticity is proven by a challenge response protocol. This protocol uses symmetric encryption and the authentication relies on the characters of the Machine Readable Zone (MRZ), a zone of two rows and 44 characters at the main data page of the passport document. The MRZ (Figure 2) contains the holder's name, nationality and birth date, the document's number and expiry date and other information depending on the issuing countries.

Figure 2 Passport data page and Machine Readable Zone (MRZ)

In order to gain access to the data stored on the RFID chip, the reader optically scans the MRZ and derives an access key out of the data contained on this page. The RFID chip also knows this key and after mutual authentication between the chip and the reader based on these symmetric keys, a cryptographic session key between the chip and the reader is derived to encrypt the data exchanged and succeed secure messaging. The authentication key is static but the session keys are different in every transaction and an incorrect key would result in denial of access [Liersch I., 2009].

So, the BAC protocol verifies that someone opened his passport and the reader scanned the MRZ and built the access key. In this way, unauthorized access is prevented [Vakalis I., 2011]. But the MRZ can be disclosed to anyone who possesses the e-passport, so the BAC protocol doesn't offer protection in case the e-passport is lost or stolen [Hornung G., 2007].

The need for even better protection of the data, when biometric data was included in the chip, led to the introduction of a new security mechanism. In 2009, the second generation of e-passports was introduced which used an Extended Access Control (EAC) system. ICAO suggested the use of EAC as an optional mechanism to provide more comprehensive authentication protocols. EAC is similar to the BAC with the difference that is uses Extended Access key instead of Basic Access Key and is based on asymmetric protocol using stronger encryption.

The EAC mechanism checks the authenticity of both the RFID chip and the reader with the use of chip and terminal authentication [Hoepman J.-H et al, 2006 & Nithyanand R., 2009]. In particular, the RFID chip is authenticated to the reader once it proves that it knows the session key and thus protects the passport from cloning (chip authentication). Then, the reader gives its digital certificate to the chip based on a public key and the chip checks its authenticity and allows its access to the stored data (terminal authentication). Terminal authentication is based upon certificate validation issued by the e-passport issuing country, so the certificates should be exchanged among countries in a secure way.

It didn't take long for the third generation of e-passports to appear as an option. The EAC offers strong benefits, but its disadvantage is that it depends on BAC and although BAC turned out to be a very successful protocol because of its simplicity

and now is implemented in almost every e-passport [ICAO Technical Report, 2010], the security that it provides is limited by the design of the protocol (the keys are cryptographically weak). So, the third generation of e-passports that use Supplemental Access Control (SAC) appeared.

SAC is based on Password Authenticated Connection Establishment (PACE v2) as a replacement to BAC. During the authentication phase, it implements asymmetric cryptography, instead of symmetric, and data encryption is based on a shared key between the reader and the chip, unlike BAC which generates the key based on the MRZ. Data is protected both when stored on the chip and when transmitted to the reader and thus higher level of protection is succeeded.

To succeed smooth migration from the one generation to the other, at border control the inspection system should support both BAC and SAC for a period of time. For the passport holders the migration will have no effect. The only thing that has to be done is to update the operating software of the inspection system.

5. E-passport vulnerabilities

To succeed better protection and security to border control more information and personal data is needed to be stored and processed. But this results in more privacy invasion too [Vakalis I., 2011]. On the one side advocates of e-passports support that e-passports offer stronger border security protecting us from terrorist attacks, but on the other side advocates of civil rights and data protection have concerns about the privacy risks [Carluccio D. et al., 2007].

Since the first e-passports appeared, several threats arose and corresponding protection mechanisms were developed. As already mentioned the RFID technology, which is used by e-passports, uses wireless communication. In the case of e-passports the operational range channel of the RFID is less than 10 cm and therefore it was assumed that the communication was relatively secure. However, these systems are vulnerable to skimming and eavesdropping by unauthorized users who possess a radio frequency reader [Hancke G.P., 2011].

Skimming attacks occur from distance when an unauthorized reader gains access to the stored data. It is an online attack where the attacker communicates directly with the RFID chip. In this case, if the data of the RFID chip is leaked, the attacker can clone the RFID chip and built a new passport.

Eavesdropping occurs when the attacker intercepts the communication between the RFID chip and the border control reader. It is an offline attack as the data is analyzed after the attack has taken place. In this situation the attacker is limited in terms of location and time since he has to be in the range of the authorized reader when the transaction is carried out [Hancke G.P., 2011].

A countermeasure proposed by ICAO to prevent clandestine scanning is to keep e-passports in a Faraday cage when not in use [ICAO Annex I, 2004]. A Faraday cage is a metal jacket that prevents any electric or magnetic fields, such those used to communicate with an RFID chip, to pass through [Ezovski G. M., 2007]. Thus, it prevents the penetration of RFID signals and as a consequence it prevents unauthorized reading too. The e-passport must be removed from the metal jacket at border control to succeed authorized reading.

Figure 3 A Faraday cage for e-passports

Another option proposed by ICAO is to place a metal surface on an adjacent page to block the chip's antenna. So the chip will not be readable while the e-passport is closed. However, passports equipped either with Faraday cages or with a metal surface on an adjacent page, are also vulnerable to eavesdropping when they are expressly presented by their holders. To overcome this problem ICAO proposed the Basic Access Control (BAC) mechanism (see chapter 4).

The BAC mechanism minimizes the risk of skimming and eavesdropping by authenticating the reader. The communication between the RFID chip and the border control reader includes protocols and encryption to succeed secure messaging. But the secret cryptographic keys are generated from the date of birth, date of expiry and passport number printed on the passport's MRZ which can be disclosed to anyone who possesses the e-passport. Thus, the BAC protocol doesn't offer protection in case the e-passport is lost or stolen and passive skimming is allowed.

6. Legal Efforts

ICAO began with the standardization of machine readable travel documents in 1968. Then, a standardized passport that would be machine readable and uses an optical character (OCR) was suggested. Later, in 1980 the recommended standards and specifications were published as the first edition of the Doc 9303 that was endorsed by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 7501-1).

The Doc 9303 evolved through time and separate volumes were published. In particular, the Doc 9303 - part 1 contained specifications about machine readable passports, the Doc 9303 - part 2 dealt with machine readable visas and the Doc 9303 - part 3 contained specifications about machine readable official travel documents alternative to passports to cross the borders.

Doc 9303 is evolving during time in line with the needs. After the attack of 9 September 2001 the need for more security at border control increased and the States decided to adopt facial recognition as a mandatory biometric and use contactless IC chips. As a result, ICAO published the Doc 9303-part 1 volume 2 in which the specifications for electronically enabled passports with biometric identification capability were presented. The biometrics, the IC contactless chips and the communication protocols (see ch. 4) were introduced.

In the meantime, the EU Council published the Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, taking into account the specifications of ICAO set out in Doc 9303. The Regulation applies only to passports and travel documents issued by the Member States (Art. 1, par. 3) and envisages that they should include a storage medium with sufficient capacity that contains a digital facial image as a first

biometric feature in a mandatory manner and fingerprints as a second biometric feature also in a mandatory way (Art. 1, par. 2).

The personal data stored in the passport is defined in the EU Directive 95/46/EC (Art. 2a), as any information that is related to an identified or identifiable natural person. Moreover, an identifiable person is one who can be identified, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. No other information shall be included in the storage medium (Art. 4, par. 2) unless it is mentioned in the passport by the issuing member state in accordance with its national legislation.

The Council Regulation refers to data protection principles too. In particular, in Art.4 par.1 the data subject's right of verification is recognized, so the e-passport holder should be able to have access to the personal data contained in his passport and even ask for rectification and/or erasure in case the data stored is incorrect. In order the data subject to be able to exercise his rights, the passport authorities must have appropriate RFID readers that allow access to the data stored on the chip and provide these readers at local places easily accessible (Kosta E., 2005 and Hornung G., 2007).

Moreover, according to Article 6 of the Council's Regulation and according to the Commision Decision C (2005) 409 of 28 February 2005, all the Member States would have to start issuing passports with a digital facial image stored in the RFID chip by 2006 and fingerprints by 2008. Pursuant to the Decision C (2005) 409, the Member States have to implement the BAC communication protocol, which is recommended by ICAO as optional, so as to safeguard access to the data stored in the chip and prevent skimming and eavesdropping.

In 2005 the ARTICLE 29 Data Protection Working Party published an opinion (3/2005) on the implementation of the above mentioned Councils' Regulation. It pointed out that the implementation of biometric features in passports raises a lot of ethic, legal and technical questions and thus the circumstances under which will be collected will have to guarantee perfect reliability. For this reason a global Public Key Infrastructure (PKI) and the creation of a Protection Profile (PP) are suggested.

7. Conclusions

During time the number of people travelling was growing rapidly and the need for more efficient and secure border control increased. In order to succeed better border security, more personal data were stored in the passports. This had the result to lead to more privacy invasion. The transition to the electronic passports was a fact since it makes travelling easier, makes the immigration inspections faster and offers stronger border security by automating identity verification.

The selection of the right technology to store the holder's personal data was a big challenge since biometric data, such as facial image and fingerprints, was also included. The International Civil Aviation Organization (ICAO) chose the RFID technology to be used as the storage medium and thus an RFID chip was embedded in the paper passport. Then ICAO published the Doc 9303 in which passport standards are issued as recommendations to the national governments and in the meantime the EU Council published the Regulation (EC) No 2252/2004 setting standards for security features and biometrics in passports issued by the Member States, taking into account ICAO's specifications. All the Member States were required to start issuing

passports with a digital facial image stored in the RFID chip by 2006 and fingerprints by 2008.

The widespread of privacy concerns used to originate mainly in the fields of law, but now has obviously expanded into the information technologies too. Since biometric data was stored on the RFID chip, serious privacy threats arose. Although RFID chips used in e-passports are equipped with protection mechanisms, they still have technical flaws and its use doesn't ensure ownership of data.

The technology's infrastructure is responsible for these problems and therefore should be enchanced with privacy enhancing technologies (PETs) to gain privacy protection [European Commission, 2007]. PETs, such as anonymisation, coding, encryption and authentication, strengthen the protection of personal data and prevent unlawful processing.

To conclude, in the case of e-passports, EU regulations and the proposed security mechanisms are not sufficient to protect privacy. The e-passport holders are still vulnerable and intensive proposed methods to enhance protection of privacy are vital. More fundamental changes are required even to the physical design of the RFID or second thoughts should be done about replacing the RFID technology with another that follows privacy principles and applies privacy by design.

To design, implement and use a technology that handles personal data and transfers them wirelessly, data protection principles have to be taken into account and privacy by design is required from the early stage of designing the technology. Therefore, the cooperation between computer and law scientists is vital for implementing a privacy enhancing technology for e-passports that entails the advantages of the RFID.

8. References

Article 29 Data Protection Working Party (2005), Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal L 385 , 29/12/2004, 1-6.

Carluccio, D., Lemke-Rust, K., Paar, C. and Sadeghi, A-R. (2007), E-Passport: The Global Traceability Or How to Feel Like a UPS Package, Information Security Applications, Lecture Notes in Computer Science, 4298, 391-404.

Cavoukian A. (1999), Privacy and biometrics, Information and Privacy Commissioner, Ontario.

Commission Decision C (2005) 409 of 28 February 2005 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States (Decision not published).

EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

European Commission Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal of the European Union.

European Commission (2007), Communication from the commission to the European Parliament and the council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final.

Ezovski G. M. (2007), The electronic passport and the future of Government-issued RFID-based identification, IEEE International Conference on RFID, 15-22.

Hancke G. P. (2011), Practical eavesdropping and skimming attacks on high-frequency RFID tokens, Journal of Computer Security, 19 (2), 259-288.

Hoepman, J., Hubbers, E., Jacobs, B., Oostdijk, M. and Schreur, R.W. (2005), Crossing borders: Security and privacy issues of the European e-passport, Lecture Notes in Computer Science, 4266, 152-167.

Hornung G. (2007), The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards, SCRIPTed, 4 (3), 246-262.

ICAO Annex I (2004), Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Version 4.0.

ICAO Doc 9303 (2006), Machine readable travel documents. Specifications for electronically enabled passports with biometric identification capability, part 1, volume 2, 6th Edition.

ICAO Technical Report (2004), Biometrics deployment of machine readable travel documents. Development and specification of globally interoperable biometric standards for machine assisted identity confirmation using machine readable travel documents, Version 2.0, ICAO TAG MRTD/NTWG.

ICAO Technical Report (2010), Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, ISO/IEC JTC1 SC17 WG3/TF5.

ICAO Working Paper (2011), Revision of the logical data structure technical report on optional expanded chip functionality, Technical advisory group on Machine Readable Travel Documents (tag/MRTD), TAG/MRTD/20-WP/3.

Juels, A., Molnar, D. and Wagner, D. (2005), Security and privacy issues in E-passports, Report, Cryptology ePrint

Kosta, E. (2006), The use of RFID chips on identification documents", Proceedings of the 2nd Greek National Conference with International Participation: Electronic democracy - challenges of the digital era, Athens, 471-480.

Liersch I. (2009), Electronic passports - from secure specifications to secure implementations, Information Security Tech. Report, 14 (2), 96-100.

National Science and Technology Council (NSTC) (2006), Privacy and Biometrics. Bulding a Conceptual Foundation, Committee on Technology, Subcommitte on biometrics.

Nikita M. (2011), RFID in the Supply Chain and the Privacy Concerns, 4th International Conference on Information Law (ICIL) 2011, Equity, Integrity & Beauty in Information Law & Ethics, Corfu – Greece.

Nithyanand R. (2009), A survey on the evolution of cryptographic protocols in epassports, Cryptology ePrint Archive, Report 2009/200.

Patil S. and Kobsa Al. (2009), Privacy Considerations in Awareness Systems: Designing with Privacy in Mind, Awareness Systems, Human-Computer Interaction Series, 2, 187-206.

Vakalis, I. (2011), Privacy and biometric passports, TheScientificWorldJOURNAL, 11, 478–489.