An analysis of security and privacy issues relating to RFID enabled ePassports

Eleni Kosta[1], Martin Meints[2], Marit Hansen[2], Mark Gasson[3]
1 K.U.Leuven, Interdisciplinary Centre for Law and ICT, Sint-Michielsstraat 6, B-3000 Leuven, Belgium, eleni.kosta@law.kuleuven.be
2 Independent Centre for Privacy Protection, Holstenstr. 98, 24103 Kiel, Germany, {meints,hansen}@datenschutzzentrum.de
3 University of Reading, Department of Cybernetics, Reading, Berkshire, UK, m.n.gasson@reading.ac.uk

Abstract. The European Union sees the introduction of the ePassport as a step towards rendering passports more secure against forgery while facilitating more reliable border controls. In this paper we take an interdisciplinary approach to the key security and privacy issues arising from the use of ePassports. We further analyse how European data protection legislation must be respected and what additional security measures must be integrated in order to safeguard the privacy of the EU ePassport holder.

1 The ePassport

Electronic ID documents are seen by the European Union as a necessary upgrade for important paper ID documents and consequently one of the first to become 'electronic' was the passport. Based on the international technical ICAO [1] standards defined in Document 9303 [2] and following Council Regulation EC 2252/2004 [3] in European legislation, the implementation of the European electronic passport (ePassport) began in 2005[1]. The ePassport is an internationally accepted Machine Readable Travel Document (MRTD) and has already been rolled out in several EU Member States.

The ICAO's Document 9303 has been adopted globally as the standard for new ePassports which ensures interoperability between regions and countries. However, adoption of the ICAO standard means that ePassports differ from the traditional passport in several ways. In order to comply with the standard, new ePassports must

[1] Note that Belgium has issued ePassports since November 2004, cf. the press release available at http://diplobel.fgov.be/en/press/homedetails.asp?TEXTID=26303

Please use the following format when citing this chapter:

Kosta, E., Meints, M., Hansen, M., and Gasson, M., 2007, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 467–472.

have a microprocessor (chip) embedded in the paper passport as well as a contactless mechanism for data transmission. For MRTDs, the ICAO specifies the use of the ISO 14443[2] standard that enables contactless data communication between the microprocessor of the ePassport and a remote reader, i.e. Radio Frequency Identification (RFID). The standard also specifies an operating frequency of 13.56 MHz and an 'intended' read range [4] of 10 to 15 cm.

For EU Member States, Art 1(2) of the Council Regulation EC 2252/2004 obliges the storage of the ePassport holder's facial image in the RFID enabled chip, whilst allowing them to "optionally also include fingerprints in interoperable formats". The biometric data are stored in the Common Biometric Exchange File Format (CBEFF), according to the standards ISO CD 19794-2 to ISO CD 19794-6.

The mechanism implemented to prevent unauthorised disclosure of digital data stored in the ePassport is Basic Access Control (BAC). The reader first acquires the Machine Readable Zone (MRZ) from the data page of the ePassport, usually via a manual optical scanner. From the MRZ data, the passport holder's birth date, the passport number and passport expiry date are used to calculate a 'session key'. This key is used to encrypt the information exchanged between reader and ePassport in order to prevent skimming of data. By using information printed on the ePassport, the intention of BAC is to restrict digitised data access to those parties who have direct physical access to the document. To prevent manipulation of the digital data, the ePassport is digitally signed by the issuing country and these signatures, which are also stored in the ePassport, can be checked during the validation of the document to ensure data integrity. Once BAC has been successfully completed, active authentication is employed to verify that the RFID enabled chip itself has not been substituted.

2 Failings of the ePassport

In short, no coherent and integrated security framework for MRTDs has been disclosed. The publicly available documentation for such a framework is currently limited to '*Protection Profiles for Biometric Verification Mechanisms and MRTDs including Basic Access Control (BAC)* [5]' and '*Technical Guideline v1.0 for Extended Access Control (EAC)*'.[3] This documentation falls short because it does not necessarily consider existing ePassport implementations[4], it consists mostly of suggestions rather than obligations and it fails to include the necessary organisational aspects of an integrated security concept. Several theoretical and scientifically demonstrated threats and conceptual flaws of ePassports have already been published, yet countermeasures have not been analysed nor specified by Protection Profiles or any appropriate technical guidelines. The most significant of these issues are further described below.

[2] Note that the ISO 14443 standard specifically refers to contactless smartcards, i.e., proximity cards which utilise RFID.

[3] Issued by the German Federal Office for Information Security (BSI) in August 2006 and announced at http://www.bsi.bund.de/fachthem/epass/eac.htm

[4] For example only the Belgian ePassports issued after July 2006 supports BAC.

Although ISO 14443 states that the distance from which the RFID enabled chip is readable should be between 10 and 15 cm, in the ePassport this can be extended [6] up to 50 or 60 cm for active communication with the ePassport and up to 5 m for eavesdropping on the ePassport / reader communication. However, most European countries have chosen not to physically shield the ePassport using a so called Faraday cage, in contrast to countries such as the U.S.

Even if the ePassport itself is physically protected, the MRZ can be easily read and copied. This is especially of concern in several countries (e.g., Italy, Slovakia and Czech Republic), where besides public authorities the passport has to be provided to private organisations, e.g., when registering in a hotel. Furthermore, BAC shows severe cryptographic weaknesses, especially the use of very low-entropy input when deriving the secret keys [7]. It has already been demonstrated that BAC in the Dutch ePassport can be circumvented (hacked) within 2 hours [6]. ISO 14443 specifies the communication protocol used between RFID enabled devices and readers. However, this communication depends on a pseudo-unique 32 bit RFID enabled chip identifier which is fixed for some implementations of the ePassport and can easily be abused to track it. Additionally, cloning of the actual RFID enabled chip in MRTDs has also been demonstrated [8].

Extended Access Control (EAC) has been proposed as an improvement to BAC, but even EAC only partially fulfils the security requirements. EAC allows an ePassport to verify the authenticity of the reader before disclosing selected elements of the personal data (notably those categorised as privacy-sensitive such as biometric fingerprint data), while data such as the digital face, name, date of birth, and so on are not covered. Furthermore, since ICAO has not accepted EAC as an international standard yet, it cannot be enforced internationally and thus non-European countries will only support BAC. Future versions of the ePassport need to be downward compatible.

Biometrics as currently implemented in MRTDs cannot be revoked. Since biometric features of the users, such as fingerprints and facial features, cannot be changed easily, 'stolen' biometrics can be abused for a long period of time. In addition, a number of methods which spoof biometric sensors have already been demonstrated [9], in some cases even without the cooperation of the person the biometric feature belongs to. The intention of European governments to further use such technologies and standards for national ID cards [10] causes additional concerns.

In summary, the use of ePassports enables tracking of citizens under certain circumstances, e.g., by equipping door frames with RFID readers, and exposes raw biometric data for additional purposes in the private and public sector. Moreover, BAC does not adequately protect the ePassport's content, while EAC is also flawed and only primarily relevant for European ePassports. Furthermore, the transfer of the ePassport's technical concept to national ID cards may well create an authentication infrastructure that is extremely vulnerable to identity theft.

3 Privacy and data protection implications of RFID in MRTDs

The data that are to be included in ePassports and that are saved on the RFID enabled chip are *information relating to an identified or identifiable natural person*, i.e., the ePassport owner, and are therefore considered as personal data according to the definition of the Data Protection Directive (hereafter DPD) [11]. This means that the European data protection legislation applies in the case of ePassports and the data protection principles must be respected. Pursuant to the data minimisation principle[5] the data stored in the RFID enabled chip shall only be those necessary for the identification of the ePassport owner.

When the ePassport is read by authorised personnel, the processing of the data stored within is legitimate since authorised personnel – and only they [12] – 'exercise official authority' (Art. 7(e) DPD). In cases of unauthorised reading of the information stored in the ePassport, such as skimming or eavesdropping, the data subject is not aware that his data are being collected. Since the data subject cannot consent to something of which he has no knowledge [13] the processing of the data is consequently not legitimate.

The ePassport owner needs to be informed about the data that will be included in the ePassport and about the ways in which he can *access, rectify, erase or block incorrect data* that are stored. Furthermore, personal data needs to be processed *fairly and lawfully* (Art. 6.1(a) DPD). The data shall be collected for specified, explicit and legitimate purposes and be further processed only in a way compatible with those purposes (finality principle) (Art. 6.1(b) DPD).

The Data Protection Directive calls the Member States to impose a security obligation on the data controller, who must implement "[...] *appropriate technical and organisational measures* to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing" (Art. 17.1 DPD). The processing of personal data must be done in a maximum security environment [14].

When considering controls carried out by authorities outside of the European Union, the use of RFID enabled chips as the storage medium on ePassports raises significant privacy concerns. When personal data are undergoing processing in a third country, this country should 'ensure an adequate level of protection', which is determined by the European Union on the basis of Article 25 (6) of the Data Protection Directive or by means of international agreements on the administrative procedures to be followed.

[5] The data shall be '*adequate, relevant and not excessive* in relation to the purposes for which they are collected and/or further processed', Art. 6.1(c) Data Protection Directive.

4 Proposed solutions

Since ePassports with the described weaknesses have already been introduced and will inevitably be used in the future, we recommend the following measures for immediate integration to reduce the risk of security failure and identity theft.

Organisational integration and enforcement of the finality principle is required, especially for biometrics used in ePassports, where the defined purpose is identification of international travellers. ePassports should not be used for authentication purposes, e.g., in the private sector. Citizens need to be informed of the risks inherent in owning, carrying and using their ePassports and the corresponding security measures which can be undertaken by them (e.g., avoiding the release of the documents to anyone, especially private organisations such as hotels, in cases when not required by law). Security measures such as Faraday cages, which are available but not widely integrated, should be integrated into newly issued ePassports immediately. In addition organisational and technical procedures are required to prevent abuse of personal data from ePassports, including tracking and identity theft.

For the next generation of the ePassport, a new convincing and integrated security framework covering MRTDs and related systems needs to be developed. It should be investigated how the integration of technologies utilised can be improved, e.g., on-card matching and on-card sensors for biometrics and it should be considered whether inherently more secure and privacy-preserving technologies such as contact instead of contactless mechanisms should in fact be used.

5 Conclusions

By failing to integrate an appropriate security architecture, European governments have effectively forced citizens to adopt new international Machine Readable Travel Documents which dramatically decrease their security and privacy and increases risk of identity theft. Simply put, the current implementation of the European passport utilises technologies and standards that are poorly conceived for its purpose. This is especially true considering the international usage and long lifetime (up to ten years) of current MRTDs. For the next generation of the ePassport a redesign including a convincing integrated security framework is needed, where most notably the use of biometrics and RFID should be reconsidered.

Acknowledgements

This paper is based in part on the 'Budapest declaration' [15] produced by the authors and other researchers from the multidisciplinary 'Future of Identity in the Information Society' (FIDIS) Network of Excellence. More detail can be found at http://www.fidis.net/. The authors would like to extend special gratitude to Danny de Cock for his valuable input to this paper.

References

1. ICAO = International Civil Aviation Organization, http://www.icao.int/.
2. Information available via http://www.icao.int/mrtd/publications/doc.cfm.
3. http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf.
4. A. Juels, D. Molnar, and D. Wagner, Security and Privacy Issues in E-passports, IEEE SecureComm 2005; available online at http://www.cs.berkeley.edu/~dmolnar/papers/RFID-passports.pdf. The term 'intended' indicates the range of vendor-standard readers.
5. Protection Profile BSI-PP-0016-2005 and BSI-PP-0017-2005, certified in August and October 2005 respectively by the German Federal Office for Information Security; available via http://www.bsi.de/zertifiz/zert/report.htm.
6. This has recently been analysed and demonstrated with a Dutch passport (see H. Robroch, ePassport Privacy Attack, 2006, which also details reading and eavesdropping distances; see http://www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf.)
7. J. Beel and B. Gipp, *ePass – der neue biometrische Reisepass,* Shaker Verlag, Aachen 2005. Download of chapter 6 "Fazit": http://www.beel.org/epass/epass-kapitel6-fazit.pdf). In most ePassports the effective key length is far lower than 56 bits, typically 35 bits, and in some cases even as low as 28 bits.
8. See, e.g., K. Zetter, Hackers Clone E-Passports, Wired News, August 3, 2006; http://www.wired.com/news/technology/1,71521-0.html.
9. Among others see Z. Geradts (ed.), *FIDIS Deliverable D6.1: Forensic Implications of Identity Management Systems*, Frankfurt 2006; http://www.fidis.net/fidis-del/period-2-20052006/#c822 / Starbug, How to fake fingerprints?, October 26, 2004; http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en.
10. In France: e.g., the project INES (identité nationale électronique sécurisée), January 31, 2005; http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050201.pdf; in Germany: C. Engel, Auf dem Weg zum elektronischen Personalausweis, Datenschutz und Datensicherheit 4/2006, pp. 207-210, Vieweg, Wiesbaden 2006.
11. 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, OJ L 281 , 23/11/1995 pp. 0031-0050.
12. Article 29 Data Protection Working Party, Opinion 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, adopted on 30 September 2001, 1710/05/EN (WP 112).
13. R. Jay and A. Hamilton, *Data protection – Law and practice*, London Sweet & Maxwell 2003, p. 91.
14. P. van Eecke and G. Skouma, RFID and Privacy: A difficult Marriage?, in: S. Paulus, N. Pohlmann, and H. Reimer (eds.), ISSE 2005 Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 2005 Conference (pp. 169-178), Vieweg, Wiesbaden 2005, p. 173.
15. http://www.fidis.net/press-events/press-releases/budapest-declaration/ (2006).