The Extended Access Control for Machine Readable Travel Documents*

Rafik Chaabouni† Serge Vaudenay

EPFL
CH-1015 Lausanne, Switzerland
http://lasecwww.epfl.ch

Abstract: Machine Readable travel documents have been rapidly put in place since 2004. The initial standard was made by the ICAO and it has been quickly followed by the Extended Access Control (EAC). In this paper we discuss about the evolution of these standards and more precisely on the evolution of EAC. We intend to give a realistic survey on these standards. We discuss about their problems, such as the inexistence of a clock in the biometric passports and the absence of a switch preventing the lecture of a closed passport. We also look at the issue with retrocompatibility that could be easily solved and the issue with terminal revocation that is harder.

1 Introduction

Since 2004, a majority of countries have adopted the ICAO standard [19, 22] for Machine-Readable Travel Documents (MRTD). It specifies how to store and use biometrics in passports to have more secure identification of the holder. Since it is based on the RFID technology [12], an access control is necessary for privacy protection. The optional one proposed in the ICAO standard is based on symmetric-key cryptography with a key printed on the passport. It is called Basic Access Control (BAC), offers very little privacy protection, and is the only mechanism which can be used to protect mandatory data groups.

Privacy is a big concern for holders. Indeed, on May 17, 2009, 49.9% of electors voted against the introduction of the biometric passport in Switzerland, presumably for privacy reasons.

To strengthen privacy, the European Union adopted an Extended Access Control (EAC) [33] to have a reasonably secure privacy protection for other data groups. It is based on public-key cryptography and requires a public key infrastructure to be deployed

*This work was partially funded by the European Commission through the ICT program under Contract ICT-2007-216676 ECRYPT II.

†Supported by the Swiss National Science Foundation, 200021-124575

for readers. Since passports are not online, they cannot receive certificate revocation lists. Thus, revocation can only be based on expiration date. Unfortunately, passports do not have a clock so they can only compare the validity period with the latest accepted certificate date.

EACv1 protects against cloning but only in the situation where it is being used in a country reading EAC. Countries reading EACv1 but being unauthorized to pass terminal authentication could use privacy-enhanced protocols, but it is not mandatory.

EACv2 may make sure that passports are only read by authorized terminals so the cloning issue may be solved. Indeed, EACv2 goes further by protecting access by EAC even ICAO-mandatory data groups, even for countries unauthorized to read other data groups. Unfortunately, ICAO-mandatory data groups must be readable by countries not implementing EAC so this protocol is likely to be bypassed for interoperability reasons.

Related work A substantial amount of work has already been achieved on MRTD. Juels, Molnar and Wagner [13] presented in 2005 one of the first (if not the first) security analysis on e-passports. They identified several flaws in the ICAO standard, namely clandestine scanning, clandestine tracking, skimming then cloning, eavesdropping, biometric data-leakage and weaknesses in the cryptographic setups of the ICAO standard. Kc and Karger [14] exposed in 2005 their research on similar tracks and introduced some other attacks, namely the "splicing" attacks and the "fake finger" attacks. In 2006, Kosmerlj et al. [15] studied the weakness of facial recognition. Hoepman et al. [11] focused in 2006 on passive attacks against BAC and gave some thoughts on biometrics. They showed that the entropy of the symmetric key used between the reader and the MRTD is less than 80 bits and can easily be guessed. Regardless of the knowledge of this secret key, they also explained how an MRTD can be traced back to individuals or groups in the classical case of skimming. Hancke [8] and Carluccio et al. [6] reported in 2006 experimental attacks against BAC. Hancke showed a practical eavesdropping together with a relay attack, and Carluccio et al. emphasized on the traceability issue of MRTD. Liu et al. [18] explained how to make a passive decryption attack. Danev, Heydt-Benjamin and Čapkun [7] demonstrated in 2009 how to uniquely identify MRTD through the physical-layer of RFID tags. They explained that this fact can help in the determination of cloned passport while on the other hand supress location privacy.

Hlaváč and Rosa [10] studied in 2007 the case of Active Authentication (AA) and presented a man-in-the-middle cloning attack against AA. AA is also subject to challenge semantics attacks as shown in [32].

Lehtonen et al. [16] proposed in 2006 a potential solution for MRTD. As a necessary optical contact has to be achieved between a reader and the MRTD, to retrieve the MRZinfo, they proposed to combine with the actual RFID chip an optical memory device. This later will enable the establishment of a secure channel as a line of sight is necessary. Hence eavesdropping and skimming will no longer be possible. Herrigel and Zhao [9] proposed to use a digital watermarking technique to increase the seed entropy which is readable by optical scanning. However the main disadvantage of these two papers is that a hardware change has to be done on passports.

Vaudenay and Vuagnoux [35] presented in 2007 a survey on existing protocols for MRTD and their corresponding weaknesses, namely the ICAO standards (BAC and AA) and the EU standard (EAC). Lekkas and Gritzalis [17] worked in 2007 on the possibility to use the ICAO standard in order to build a globally interoperable Public Key Infrastructure. However they came up with negative conclusions due to several lacks such as the lack of passport revocation mechanism. Pasupathinathan, Pieprzyk and Wang [28, 29, 30] achieved in 2008 a formal security analysis on the Australian e-passport and identified several flaws in EACv1, after which they proposed an enhanced version called OSEP. They introduced the need to execute terminal authentication before chip authentication. Abid and Afifi [1] in 2008 incorporated in OSEP the use of elliptic curves.

All these research pushed the "Bundesamt für Sicherheit in der Informationstechnik", in charge of the EAC standardization, to present a new version (EACv2) in October 2008 and to add minor changes in May 2009 (version 2.01).

Nithyanand [27] released in 2009 a first survey on EACv2, that claimed that EACv2 solved all the previous problems except the vulnerability of reading a passport with an outdated date by a reader with an expired certificate. Unfortunately this is not the only problem left with EACv2.

Monnerat, Vaudenay and Vuagnoux [25] focused in 2007 on the privacy concerns attached to the release of passport Security Object Document (SOD). It leaks the hash of protected data groups and also evidence on private data. (See also [34]) Monnerat, Pasini and Vaudenay [24] constructed in 2009 an Offline Non-Transferable Authentication Protocol to achieve a Zero-Knowledge proof of knowledge of a valid SOD.

Structure of the paper The aim of this paper is to provide a general survey on the MRTD standard evolution and explain what are the remaining problems. Moreover we will propose directions for the next generation in order to suppress these problems. We will first explain and give the drawbacks of the RFID, the ICAO standard, the EACv1 and the EACv2 respectively in section 2, 3, 4 and 5. In section 6 we will provide our potential solutions and conclude in section 7.

2 ISO Standard for RFID

In order to discover the RFID tags in proximity, according to the ISO standard for RFID [12], readers send a discovery signal. Any RFID tag receiving this signal will reply with a specific identifier in order to allow readers to enter in communication with them. For regular RFID tags, this identifier is constant to enable an easy way to track chips. However this property is not always desirable for tags especially when location privacy needs to be protected. This the case for MRTD. The solution proposed by the ISO standard is to use a session-dependent randomly generated identifier. This solution has been adopted by almost all countries. Unfortunately, there are discrepancies in the way it is implemented [25]. There are other protocol implementation differences such as availability of optional features, lower layer protocols ar speed of transmission which allow to identify a passport

nationality [35].

It is a well known fact that privacy must be addressed accross all protocol layers [4]. As a matter of fact, recent work by Danev et al. [7], shows that any RFID tag can be accurately identified according to his physical-layer communication properties, namely by some kind of radio fingerprint. Although their work uses this property to enable cloning detection, the straightforward drawback is the tag tracking possibility.

Furthermore, the distance to eavesdrop or to interact with RFID tags is highly underestimated. According to an announcement from the Swiss Federal Office of Communication (OFCOM) [2] in November 2008, and even though currently commercialized readers can interact only within few centimeters, it would be possible by changing readers antenna to access MRTD from far away (up to 25 meters). In addition to this, radio communication between a legitimate reader and a passport induce a signal on the power line and can be captured 500 meters away.

3 ICAO Standard and BAC

Following the ICAO standard, passports must provide passive authentication for two mandatory data groups:

- Data group DG1 is a digital copy of the printed Machine Readable Zone (MRZ) which included some basic information about the holder: name, nationality, gender, date of birth, as well as passport serial number and expiration date.
- Data Group DG2 is a digital picture of the face which is optimized for automatic face recognition.

Passive authentication is performed by means of the Security Object of the Document (SOD), which is essentially a digital signature of the list of the hash of data groups together with the certificate of the verifying key. This certificate is computed by the issuing country and the root verifying key of the PKI is assumed to be authenticated by special protocols. Following the state of the art on cryptography, digital signatures are unforgeable so identities can no longer be forged by malicious people.

Biometric identification is mostly performed by 2D facial recognition, and soon by fingerprint as well. It could use iris recognition but this technology does not seem to be implemented yet. One problem is that 2D-facial recognition is pretty weak and that fingerprint could be fake. Fake fingerprint can be made using candy [23] or medecine against constipation [5].

Passports could limit themselves to providing DG1, DG2, and SOD in a pretty passive way. Indeed, it could have been printed using 2D barcode. But ICAO preferred RFID-based technology to accommodate more data and functionalities. Radio access then opened the way to privacy threats and require passports to implement some access control.

The ICAO standard includes an optional Basic Access Control (BAC), based on 3DES [3], which essentially consists in making the reader prove that it knows some piece of infor-

mation on the printed MRZ. This information called MRZinfo consists of the passport serial number, the date of birth of the person, and the expiration date of the passport. That is, BAC uses symmetric-key cryptography with an access key which is printed on the passport. Furthermore, MRZinfo has a pretty low entropy (following [20], an entropy of roughly 56 bits). So far, BAC is implemented in every passports we have seen.

BAC is followed by some key agreement to open secure messaging. Again, it is all based on symmetric cryptography with a low-entropy initial key (the MRZinfo), so it does not resist to passive adversaries.

The ICAO standard also includes an optional Active Authentication (AA) protocol which is based on a digital signature scheme. It protects against cloning attacks but is time-consuming for the powerless chip. As far as we know, it is only implemented in Belgium and the Czech Republic. Moreover AA is not secure against man-in-the-middle attacks [10] and leads to privacy concerns by adding semantics within the challenge [33].

Clearly, the advantages of the ICAO passports is that identities are unforgeable and that access to the chip requires knowing MRZinfo. Unfortunately, there are many drawbacks.

First of all, the cryptographic protocols do not resist passive adversaries. Since AA is seldom used, it does not resist to cloning attacks. Furthermore, MRZinfo grants an unlimited permanent access: once the adversary gets it, she can access to the chip without the consent of the holder. Contrarily to popular belief, the release of DG2 and SOD is not privacy insensitive. Releasing DG2 means releasing an optimized picture which is used as a reference template for biometric recognition. Once an adversary gets it, he can train himself to match the template, so releasing DG2 can ease identity theft. Hence the assumption 2.3 in section IV of [20] is wrong.

> The digitally stored image of the face is assumed not to be privacy-sensitive information. The face of the MRTD holder is also printed in the MRTD and can be readily perceived.

In addition to this, releasing SOD means providing transferable evidence of the correctness of the identity. For instance, it could be used as an undeniable proof for true date of birth for someone who tries to make his age a taboo.

4 EAC v1

The European EAC standard [32] was made to add better protection for non-mandatory data groups such as DG3: the fingerprint template. It includes

- secure messaging based on ECDH [31];
- a chip authentication protocol, protecting against cloning attacks;
- a terminal authentication protocol.

Terminal authentication is meant to be mandatory for accessing non-mandatory data groups, but mandatory data groups must remain readable without EAC due to the ICAO standard.

In the terminal authentication protocol, the reader proves that he owns the secret key associated to a given public key. Typically, this proof consists of signing a challenge from the passport. The public key has a certificate chain whose root belongs to the home country of the passport. That is, authorization is given to readers by signing a certificate with a given validity period. One problem is that passports do not have any reliable clock. So, they keep in memory a trusted past date which plays the role of a clock. When they check the validity of a certificate, they just check that the expiration date is posterior to the clock value. If verification succeeds and the issuing date of the certificate is posterior to the clock value, the clock value is replaced. Clearly, passports which do not run terminal authentication often will not even have a reliable approximation of a clock. Others may have a date which is precise within a few weeks. Consequently, a terminal certificate may be usable a long time after expiration to read passports.

The details of the general PKI required to authenticate readers at terminal station is described in the EACv2 standard [33].

The advantage of EAC is that we now have anti-cloning protection, a better key agreement resisting passive adversaries, and we can handle time-limited privileges to different readers. A problem is that revocation is based on a pretty weak clock. We still have privacy issues related to releasing DG2 and SOD to anyone. Also, the hash of protected data groups leaks from the SOD [33].

5 EACv2

EACv2, released in 2008 then updated in May 2009, describes among other specifications the PKI for terminals. This PKI is composed of three types of entities, namely Country Verifying Certificate Authorities (CVCAs), Document Verifiers (DVs) and Terminals. Every country will be required to have its own CVCA issuing MRTD and DV Certificates. DVs are organizational units within countries. Their role is to enable the certification link between its terminal readers and CVCAs. Hence they need to apply for a DV Certificate at each CVCAs corresponding to the country of MRTD that might be encountered by its Terminals. DVs are also in charge of creating and maintaining Terminal Certificates for each Terminal location. The validity period and the access rights of the terminal certificate are inherited from the DV Certificate. Obviously, these restrictions can be further reduced by the decision of the DV in charge of the terminal. Equivalently, the validity period and the access rights contained in the DV certificate is decided by the CVCA issuing the certificate.

The access rights for all data groups is encoded in binary in each certificate as an object identifier according to the role of the certificate holder (inspection systems, authentication terminals or signature terminals). A member in the certificate chain cannot provide more access rights than what it has itself. Thus to determine the access rights of a partic-

ular reader, the MRTD has to compute the boolean AND of all the binary authorization contained in the certificate chain.

EACv2 resolves one of the issue of EACv1, namely the privacy issue linked to releasing DG1, DG2, and SOD. The main difference introduced is in the order of authentication between a chip and the terminal that is attempting to read it. In this new specification the terminal authentication must be performed before the chip authentication. EACv2 even introduces a replacement for BAC, namely PACE. PACE is a state-of-the-art password-based access control resisting active attacks. Another improvement is that the access password for PACE is now a specific secret printed inside the passport and no longer any private data which has other purposes such as MRZinfo.

This modification could be considered at a first glance as a major improvement. Indeed by forcing authentication of the terminal before the chip authentication, we restrict the release of DG2 and SOD only to officially allowed terminals. However this is not the case in a full view of the specifications. By reading carefully the specifications of the EACv2 in [33], we can read in section 3.1.1 the following note:

> **Note:** According to this specification it is RECOMMENDED to require Extended Access Control to be used even for less-sensitive data. If compatibility to ICAO [20, 21] is REQUIRED, the MRTD chip SHALL grant access to less-sensitive data to terminals authenticated by Basic Access Control. The relevant inspection procedures are described in Appendix G.

What this note states is that if compatibility to ICAO is required then the MRTD must behave as in the ICAO standard. In other words, any fake terminal reader can require from the MRTD to use the crippled ICAO standard.

Furthermore the date contained in the MRTD is still an approximation of the current date. The date is updated only with national domestic certified dates, i.e. certificate effective dates (date of the certificate generation), contained in a national domestic CVCA certificate, a DV authorization certificate issued by the national domestic CVCA, or an accurate terminal certificate, i.e. a terminal certificate issued by an official domestic DV. As an MRTD will rarely encounter a domestic terminal, it is more likely that its date will be updated through the certificate effective date contained in a foreign DV. Hence the revocation of terminals is not fully solved.

6 Directions for the Next Generation

RFID switch In order to avoid traceability of passports, the current solution that people have is to place their MRTD in a faraday cage. Obviously this solution is cumbersome. For the case of biometric passport a better solution would be to incorporate an RFID switch to desactivate the chip. Some sensors could also detect if the passport is opened or closed and manipulate the switch accordingly. When the passport is closed the RFID tag

would simply ignore all discovery signals sent by readers and in order to interact with the passport, the later would need to be opened. This solution is logical as the access password for PACE printed inside the passport is supposed to be scanned by border patrols.

BAC abolishment Several changes need to be brought in the current EACv2 specifications. The fist element to take into consideration is that BAC should be abolished. In order to comply with the ICAO standard, the later should stop mandating DG1, DG2 and SOD available without EAC. EAC has to be imposed outside Europe in order to fully deploy its capacity. As for the EAC and ICAO standards, it only requires dropping a few lines in the documents.

Deployment does not necessarily imply a heavy PKI for terminals. A country not ready to have such a PKI could still use a dummy one with a single key shared to all readers. The passport issuing country, aware of it, could adjust the read access to mandatory data groups and keep the possibility to stop renewing a certificate for this key if the reading country does not make enough efforts to avoid leakage of the secret key. EAC-reading is a matter of software update and is inexpensive. Therefore, the only obstacle to making pure EAC mandatory is purely political.

Time-based revocation To be more accurate on the date contained in the MRTD, we propose to have identity checks even when leaving a domestic country or a community space if the community space members trust each others. For instance, some domestic clock-update booths could be made available on a voluntary basis before departure. As the identity check will correspond to an interaction with an accurate terminal, the date in the MRTD will be updated with the terminal certificate effective date. The date contained in the MRTD is still an approximation in this scenario, however with reduced date error when compared to EACv2. Finally, future chips might be equipped with a real clock.

Repetition-based revocation To decrease the issue of terminal corruption, terminal authentication could be improved by using reputation-based trust mechanisms. For instance the current terminal authentication would be appended by a $(t, n, \tau, \eta)-$threshold authentication proof, where a terminal can authenticate itself only if it collaborates with t neighbor connected terminals out of n and τ DV out of η. After completion of their proof, terminals should not be able to become offline for next authentication proofs. This add-on will resolve the problem of a single stolen terminal as a malicious party will have to corrupt at least t terminals and τ DV. However note that this solution does not resolve the case where a whole country is corrupted and no more trusted.

The ultimate trust mechanism would be an authentication proof involving the home CVCA. That is, passport would communicate to their own authority to check revocation status (like OCSP [26]).

7 Conclusion

In conclusion we can attest on the improvement brought by EACv2 with their new specifications. However further work is still needed. For instance as retrocompatibility is enabled in the MRTD to use ICAO with BAC instead, the whole security meaning behind EAC falls. The last issue concerns terminal revocations. Due to the inexactitude of date in MRTD, a terminal can fake its authentication even after its expiration date in his certificate. The frequency of date modification in MRTD is clearly not enough. A solution may be based on a threshold authentication proof in terminal authentications. Maybe future technologies will make it possible to have a real clock in passports, which would make easier solutions feasible.

Another remaining big concern relates to the overall RFID technology. Currently, it is easy to distinguish passports from different countries without any direct contact. The only way to protect against it is to prevent the chip from responding. That is, an on/off switch must be missing, or at least a sensor which switches off the chip when the passport is closed.

References

[1] M. Abid, H. Afifi. Secure E-Passport Protocol Using Elliptic Curve Diffie-Hellman Key Agreement Protocol. In *Proceedings of the 2008 The Fourth International Conference on Information Assurance and Security (IAS'08)*, Washington, DC, USA, pp. 99–102, IEEE, 2008.

[2] Abklärungen über die Datenauslesung auf Distanz beim biometrischen Pass. *Bundesamt für Kommunikation BAKOM*, 28 November 2008. `http://www.schweizerpass.admin.ch/etc/medialib/data/passkampagne/e-paesse.Par.0004.File.tmp/Messbericht_Bakom.pdf`

[3] ANSI X9.52. Triple Data Encryption Algorithm Modes of Operation. ANSI. 1998.

[4] G. Avoine, P. Oechslin. RFID Traceability: A Multilayer Problem. In *Financial Cryptography and Data Security, 9th International Conference (FC 2005)*, Roseau, The Commonwealth of Dominica, Lecture Notes in Computer Science 3570, pp. 125–140, Springer-Verlag, 2005.

[5] C. Barral, A. Tria. Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin. In *Formal to Practical Security: Papers Issued from the 2005-2008 French-Japanese Collaboration*, Lecture Notes in Computer Science 5458, pp. 57–69, Springer-Verlag, 2009.

[6] D. Carluccio, K. Lemke-Rust, C. Paar, A.-R. Sadeghi. E-Passport: The Global Traceability or How to Feel Like an UPS Package. In *Information Security Applications (WISA'06)*, Juju Island, Korea, Lecture Notes in Computer Science 4298, pp. 391–404, Springer-Verlag, 2007.

[7] B. Danev, T.S. Heydt-Benjamin, S. Čapkun. Physical-layer Identification of RFID Devices In *Proceedings of the 18th USENIX Security Symposium (USENIX'09)*, Montreal, Canada, pp. to appear, USENIX, 2009.

[8] G.P. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, Berkeley, CA, USA, pp. 328–333, IEEE, 2006.

[9] A. Herrigel, J. Zhao. RFID identity theft and countermeasures. *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, vol. 6075, pp. 366–379, 2006.

[10] M. Hlaváč, T. Rosa. A Note on the Relay Attacks on e-Passports: the Case of Czech e-Passports. Technical reports 2007/244. IACR.
http://eprint.iacr.org/2007/244

[11] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, R. Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In *Advances in Information and Computer Security, First International Workshop on Security (IWSEC'06)*, Kyoto, Japan, Lecture Notes in Computer Science 4266, pp. 152–167, Springer-Verlag, 2006.

[12] ISO/IEC 14443. Identification Cards — Contactless Integrated Circuit(s) Cards — Proximity Cards. ISO. 2001.

[13] A. Juels, D. Molnar, D. Wagner. Security and Privacy Issues in E-Passports. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05)*, Washington, DC, USA, pp. 74–88, IEEE, 2005.

[14] G. S. Kc, P. A. Karger. Preventing Attacks on Machine Readable Travel Documents (MRTDs). *Cryptology ePrint Archive*, Report 2005/404.

[15] M. Kosmerlj, T. Fladsrud, E. Hjelmås, E. Snekkenes. Face Recognition Issues in a Border Control Environment. In *Advances in Biometrics, International Conference (ICB 2006)*, Hong Kong, China, Lecture Notes in Computer Science 3832, pp. 33–39, Springer-Verlag, 2006.

[16] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch. Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. Presented at *Developing Ambient Intelligence: Proceedings of the First International Conference on Ambient Intelligence Development (Amid'06)*, 2006. In *Developing Ambient Intelligence: Proceedings of the First International Conference on Ambient Intelligence Development (Amid'06)*, Sophia Antipolis, France, pp. 253–267, Springer, 2006. to appear in International Journal of Information Security (IJIS)

[17] D. Lekkas, D. Gritzalis. E-Passports as a Means Towards the First World-Wide Public Key Infrastructure. In *Public Key Infrastructure, 4th European PKI Workshop: Theory and Practice (EuroPKI 2007)*, Palma de Mallorca, Spain, Lecture Notes in Computer Science 4582, pp. 34–48, Springer-Verlag, 2007.

[18] Y. Liu, T. Kasper, K. Lemke-Rust, C. Paar. E-Passport: Cracking Basic Access Control Keys. In *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS (OTM Confederated International Conferences CoopIS, DOA, ODBASE, GADA, and IS 2007)*, Vilamoura, Portugal, Lecture Notes in Computer Science 4804, pp. 1531–1547, Springer-Verlag, 2007.

[19] Machine Readable Travel Documents. Development of a Logical Data Structure — LDS For Optional Capacity Expansion Technologies. Version 1.7. International Civil Aviation Organization. 2004.
http://www.icao.int/mrtd/download/technical.cfm

[20] Machine Readable Travel Documents. Part 1: Machine Readable Passport, Specifications for Electronically enabled Passports with Biometric Identification Capabilities. International Civil Aviation Organization. ICAO Doc 9303, 2006.
http://www2.icao.int/en/MRTD/Pages/default.aspx

[21] Machine Readable Travel Documents. Part 3: Machine Readable Official Travel Documents, Specifications for Electronically enabled Official Travel Documents with Biometric Identification Capabilities. International Civil Aviation Organization. ICAO Doc 9303, 2008. http://www2.icao.int/en/MRTD/Pages/default.aspx

[22] Machine Readable Travel Documents. PKI for Machine Readable Travel Documents offering ICC Read-Only Access. Version 1.1. International Civil Aviation Organization. 2004. http://www.icao.int/mrtd/download/technical.cfm

[23] T. Matsumoto. Gummy and Conductive Silicone Rubber Fingers. In *Advances in Cryptology, 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2002)*, Queenstown, New Zealand, Lecture Notes in Computer Science 2501, pp. 574–576, Springer-Verlag, 2002.

[24] J. Monnerat, S. Pasini, S. Vaudenay. Efficient Deniable Authentication for Signatures. In *Applied Cryptography and Network Security, 7th International Conference (ACNS 2009)*, Paris-Rocquencourt, France, Lecture Notes in Computer Science 5536, pp. 272–291, Springer-Verlag, 2009.

[25] J. Monnerat, S. Vaudenay, M. Vuagnoux. About Machine-Readable Travel Documents: Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication. In *International Conference on RFID Security 2007*, Málaga, Spain, pp. 13–26, University of Málaga, 2008.

[26] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. 1999 *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. RFC. RFC Editor.

[27] R. Nithyanand. The Evolution of Cryptographic Protocols in Electronic Passports. *Cryptology ePrint Archive*, Report 2009/200.

[28] V. Pasupathinathan, J. Pieprzyk, H. Wang. Formal Security Analysis of Australian E-passport Implementation. In *Sixth Australasian Information Security Conference (AISC 2008)*, Wollongong, NSW, Australia, pp. 75–82, ACS, 2008.

[29] V. Pasupathinathan, J. Pieprzyk, H. Wang. An On-Line Secure E-Passport Protocol. In *Information Security Practice and Experience, 4th International Conference (ISPEC 2008)*, Sydney, Australia, Lecture Notes in Computer Science 4991, pp. 14–28, Springer-Verlag, 2008.

[30] V. Pasupathinathan, J. Pieprzyk, H. Wang. Security Analysis of Australian and E:U: E-passport Implementation. *Journal of Research and Practice in Information Technology*, vol. 40, num. 3, pages 187–205, 2008.

[31] SEC 1: Elliptic Curve Cryptography. v1.0, Certicom Research, 2000. http://www.secg.org/secg_docs.htm

[32] Technical Guidelines TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents — Extended Access Control (EAC). Version 1.11. Federal Ministry of the Interior. Bundesamt für Sicherheit in der Informationstechnik. 2008.

[33] Technical Guidelines TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents — Extended Access Control (EAC). Version 2.01. Federal Ministry of the Interior. Bundesamt für Sicherheit in der Informationstechnik. 2009.

[34] S. Vaudenay. E-Passport Threats. *IEEE Security & Privacy*, vol. 5, num. 6, pages 61–64, 2007

[35] S. Vaudenay, M. Vuagnoux. About Machine-Readable Travel Documents. *Journal of Physics: Conference Series*, vol. 77, num. 012006, 2007. http://www.iop.org/EJ/article/1742-6596/77/1/012006/jpconf7i_77_012006.pdf