# About Machine-Readable Travel Documents

Serge Vaudenay and Martin Vuagnoux

EPFL, Lausanne, Switzerland
http://lasecwww.epfl.ch

**Abstract.** Passports are documents that help immigration officers to identify people. In order to strongly authenticate their data and to automatically identify people, they are now equipped with RFID chips. These contain private information, biometrics, and a digital signature by issuing authorities. Although they substantially increase security at the border controls, they also come with new security and privacy issues. In this paper, we survey existing protocols and their weaknesses.

## 1 Introduction

The UN International Civil Aviation Organization (ICAO) started to work on Machine-Readable Travel Documents (MRTD) in 1968. In 1980, the first standard specifies a discrete Machine-Readable Zone (MRZ) to be optically scanned. It contains basic information such as the document number, its expiration date, the name, gender, date of birth, and citizenship of the person. It is now being used in many identity documents, such as passports. Since 1997, ICAO works on adding more data, including biometrics. To do so, optical memories have insufficient capacity. To further avoid physical contact and better ease of use, a contactless IC chip was preferred. Their memory capacity makes it possible to host digital pictures, biometric templates, and authentication by strong cryptographic means. In 2004, the first version of the standard was released, under pressure by the need to strengthen border controls after 2001 9/11.

As minimal requirements, MRTD must provide a facial image, a digital copy of the MRZ, and to have them digitally signed by the issuing country. The digital signature comes with a Public-Key Infrastructure (PKI). The ICAO standard provides

- a passive authentication protocol to authenticate the data
- an optional Basic Access Control (BAC) so that the chip content is protected gainst unauthorized access
- an Active Authentication (AA) to prove that the chip is genuine.

BAC offers little security, but the standard lets open the development of Extended Access Control (EAC). This is precisely what is being developed and standardized at the European level. Similarly, weaknesses in AA are also reported.

*Previous work.* The concept of e-passport was introduced by Davida and Desmedt [6,7] in 1988. One of the first study on privacy issues from RFID protocols, including singulation ones, is due to Avoine and Oechslin [1]. In 2005, Juels, Molnar and Wagner [14] presented a survey on MRTD and RFID. Among other issues, they discussed about the "biometric threat" and shortcomings in the Basic Access Control (BAC) protocol. In 2006, Hoepman et al. [13] discussed more about unauthorized access and skimming over the BAC protocol. They studied the entropy of the access key. They also discussed about the EU Extended Access Control (EAC). They detailed a revocation issue related to terminal authentication. They further discussed on biometrics. An experimental attack based on the BAC weaknesses was reported in 2006 by Hancke [11] and Carluccio et al. [5]. In 2006, Lehtonen

et al. [15] studied ways to make optical memory and contactless IC chip interact for the benefit of security. Hlaváč and Rosa have demonstrated a man-in-the-middle attack on Active Authentication in 2007 [12]. Finally, Monnerat et al. have discussed on transferability of digital evidence and studied ways to fix it [18].

## 2 The ICAO Standard

The ICAO normative document is called *Document 9303*. The 6th edition, the latest version from 2005, does not include (yet) the PKI and LDS standards which are specified in separate documents. The LDS standard [16] describes the LDS, the on-board operating system, and the communication protocol to the IC chip. The PKI standard [17] concentrates on cryptographic aspects. Here, we refer to these documents as the *ICAO standard*.

*Machine Readable Zone.* The MRZ contains: the document type (e.g. "passport"), the issuing country code, the holder name, the document number, the nationality of the holder, his date of birth, his gender, the expiry date of the document, and several options which are left up to the issuing country. Below is a (forged) example of MRZ for Mr Jean Dupont, born on April 1st 1973, citizen of France with a passport number 74HK8215 issued by Switzerland expiring on May 12 2007:

```
PMFRADUPONT<<<<JEAN<<<<<<<<<<<<<<<<<<<<<<<<
74HK8215<6CHE7304017M0705121<<<<<<<<<<<<<<03
```

*Logical Data Structure.* The LDS files are called Data Groups (DG) and numbered from DG1 to DG19. Data group DG1 is the digital version of the MRZ. Data group DG2 is a facial digital picture. It is optimized for automatic face recognition. These are the only mandatory data groups. Data group DG15 is the public key of the chip when AA is implemented. Some other data groups can accommodate templates for digital fingerprint, iris image, written signature and other personal information (e.g. the place of birth, etc). Data groups DG1 to DG15 must be authenticated by means of passive authentication as detailed below. In addition to data groups, an extra file called Security Object for the Document (SOD) is provided. Some other files are not accessible as they contain secret keys.

The SOD lists the hash of all data groups and a signature of this list by the issuing Document Signer (DS) who produced the MRTD. The certificate of the DS public key may also be provided in the SOD. If not present, this certificate can be obtained from the ICAO directory.

Each country has its own PKI. The root self-signed certificate is transmitted to all other countries by diplomatic means. In addition to this, a revocation procedures specifies that Certificate Revocation Lists (CRL) may routinely be issued every 3 months and that alert CRL must be issued within 48 hours upon discovery of a key corruption.

The LDS structure specifies Data group DG16 (which is not listed in SOD, thus not authenticated) to store contact person to notify (presumably for the passport of children or persons requiring assistance). Other data groups are left for visiting countries to store electronic visa, automatic border clearance, or travel records. This means that reader may use the IC chip to store or modify data. Although we have not been able to check, it is likely that such intrusive access may be conditioned to strongly authenticating the reader by means which are not standardized in the ICAO standard yet.

*Passive authentication.* Passive authentication is done by means of a digital signature scheme. Table 1 lists the signature algorithms which are used to sign the DS certificate, to sign the SOD, and the signature algorithm in AA.

**Table 1.** Signature Algorithms (with signature length).

| | certificate | SOD | AA |
|---|---|---|---|
| Switzerland | ecdsa_with_sha1 (824b) | ecdsa (512b) | n/a |
| United Kingdom | sha256withRSA (4096b) | RSA (2048b) | n/a |
| Czech Republic | rsaPSS (3072b) (using sha1) | RSA (2048b) | RSA (1024b) |
| Belgium | sha1withRSA (4096b) | RSA (2048b) | ? |
| Germany | ecdsa_with_sha1 (560b) | ecdsa (464b) | n/a |
| Italy | sha1withRSA (4096b) | RSA (2048b) | ? |
| New-Zealand | sha256withRSA (4096b) | RSA (2048b) | ? |
| USA | sha256withRSA (4096b) | RSA (2048b) | ? |

*Basic Access Control.* BAC is used for several objectives. First of all, it checks whether the reader is authorized to access to the chip content. To do so, the reader proves that it knows a subset of the MRZ called MRZ_info. The idea behind is that one should not know the MRZ without opening the passport, and opening the passport would mean that the holder authorized to read it. The MRZ_info consists of the document number, the date of birth and the expiry date. In our MRZ example, there are `74HK821` , `730401` and `070512` , respectively.

Second, BAC completes a key agreement protocol between the reader and the chip to derive a symmetric and private session key. The key agreement protocol is made from the 3DES algorithm and based on MRZ_info. Contrarily to regular key agreement protocols, it is not immune to passive attacks when MRZ_info is known. Contrarily to password-based authenticated key agreement, it is not even immune to offline exhaustive search if MRZ_info has little entropy (which is often the case).

Finally, the BAC exchanged key is used for secure messaging so that communication between the chip and the reader is protected based on the 3DES algorithm. Secure messaging consists of an encrypt-then-authenticate protocol where encryption uses 3DES with two keys and authentication is a kind of CBCMAC followed by encryption which resembles to 3DES with two keys as well. Overall, the secure messaging symmetric key consists of 224 bits.

Ideally, BAC should protect against passive eavesdropping: what is called *data skimming*.

The key agreement works as follows. Firstly, a symmetric key is (deterministically) derived from MRZ_info by using the SHA1 algorithm to open secure messaging. Secondly, there is an explicit mutual authentication to check that secure messaging is working well. Finally, two random numbers are exchanged, and the XOR of the two numbers serves as a new seed to derive session-dependent symmetric keys for secure messaging. More concretely, a random number RND.ICC is sent in clear from the chip to the reader. The reader must answer by sending (through secure messaging) a string containing RND.ICC, a new random number RND.IFD, and an other random number K.IFD. The chip must answer by sending (through secure messaging) a string containing RND.IFD, RND.ICC, and a new random number K.ICC. The final seed is the XOR of K.ICC and K.IFD.

*Active Authentication.* Without AA, someone who has access to an e-passport could easily dump the memory and make a clone of the IC chip. AA is used to prove that the chip is not a clone. Concretely, a digital signature scheme is used. Its public key is data group DG15 and authenticated from passive authentication. The secret key never leaves the chip. To prove knowledge of the secret key, the reader sends a challenge to the chip and the chip signs it. The reader can check the signature. If the signature is unforgeable, this is a sound proof of knowledge.

*Overall identification procedure.* To identify a traveler, the inspector proceeds as follows.

1. The inspector opens the e-passport and makes its MRZ scanned by his terminal.

2. His reader accesses to the IC chip through radio channel.
3. In the case of access denied by the chip, the reader and the chip run BAC based on MRZ_info.
4. The reader loads the SOD, checks the certificate, checks the signature.
5. The reader loads DG1, checks its hash from SOD, and checks it matches the optically scanned MRZ.
6. If AA is supplied, the reader and the chip run AA.
7. The reader loads DG2, checks its hash from SOD, and does automatic face recognition with the traveler.
8. Perform further biometric identification if supplied.

The inspector should still check whether the e-passport looks genuine and that the information matches what its device infers.

## 3 Security and Privacy Issues in the ICAO Standard

We review here known security and privacy issues regarding the ICAO standard.

*The RFID singulation protocol.* When a reader queries for alive RFID tags, several can answer at the same time. To resolve collisions, a singulation protocol is used. Typically, all tags will announce their 32-bit identifier and the reader will decide to which it wants to talk. E-passports from New Zealand and Italy use a constant 32-bit identifier so they can easily be tracked by spying sensors.

Following the ISO 14443 standard, tags can use either a fixed 32-bit identifier or a random one starting with by `08`. Using a random identifier is a privacy protection. Unfortunately, their is a discrepancy between tags requiring privacy protection and tags do not taking care of privacy. This means that tags with an identifier starting with by `08` are likely to be privacy-sensitive tags. They can thus be identified as a potential target by spying sensors.

For that reason, some countries like Australia (and presumably USA) decided to use a true 32-bit random identifier, i.e. not to follow the ISO 14443 standard. This is quite an odd decision because it may have the exact opposite effect: tags identifying themselves with an ever-changing 32-bit number not starting with byte `08` are more likely to be e-passports from Australia or countries following the same strategy, thus a most valuable target for passport thieves.

Indeed, privacy protection standards in RFID should be universally followed, even by tags not requiring any privacy protection. This could ideally work provided that all tags use the same hardware and implementation. Otherwise, their radiation pattern signature would leak [10]. Privacy issues coming from communication protocol layers is discussed in [1].

*RFID shields.* Radio access to the IC chip is the source of many privacy issues. Even though there was a strongly secure access control protocol (which is not the case of BAC as discussed below), sensors could still detect the presence of tags (if not e-passports as already discussed). This is done by sensors doing unauthorized scanning. To solve this problem, one could use a shield around the IC chip. For e-passport, it is pretty easy to put a metallic cover playing the role of a Faraday cage when the passport is not opened. Opening the passport assumes the agreement by the holder to scan the chip. As far as we know, this approach was adopted by the USA only.

One cited drawback of this approach is that shielded e-passports make security gates ring, leading the traveler to the additional burden of having his passport off (together with coins, watches, belts, cell phones, shoes, and liquids) when passing through the gate.

*Basic Access Control.* Rough estimates of the MRZ_info leads to the straightforward observation that exhaustive search is feasible. If the document number, expiration date, and birth date of the holder were purely random, the entropy would reach 70 bits. But this is not the case since visual contact can easily reduce the set of possible birth dates. Furthermore, the document numbering scheme of every countries leads to poor entropy. Most of countries use consecutive numbers in interval reserved to every issuing agencies. Thus, the knowledge of the scheme and existing numbers melt the entropy down to slightly more than 30 bits. One estimate calculation is detailed in [13].

As pointed out in [14], online bruteforce attack on BAC can be run within a few hours during which a reader connects to the IC chip with guesses on the MRZ_info. Alternatively, passive eavesdropping of the communication between an authorized reader and the IC chip can lead to offline bruteforce attack that will lead to decrypting all communications.

In practice, those attacks are not easy from a technological viewpoint. Standard RFID readers can connect to the IC chip up to a distance of 5cm with the chip well aligned to the reader. It makes sense to assume that pirate reader might work up to a few meters. However, the reader shall to be too far away because the power used by the IC chip to run calculation and to answer is taken from the reader signal. If a power source (e.g. a legitimate reader) is close to the IC chip, we can still assume that communication from the reader can be captured from pretty far away. Getting the communication from the IC chip is more difficult since the signal power is weaker. One experiment is detailed in [5,11].

We can still try to push the attack to further distance limits. Indeed, when an e-passport is being accessed by a legitimate reader and the adversary can hear the communication from the reader only, one can observe that the first encrypted BAC message from the reader is a redundant message that is encrypted and authenticated with a symmetric key derived from the MRZ_info only. This is far enough to recover MRZ_info by exhaustive search. Once MRZ_info is obtained, the adversary can try to get closer to the pocket of the holder to run BAC and dump the chip content.

In the current state of the art of cryptography, we do not know how to design a key agreement protocol that resists to passive adversaries when no public-key cryptography technique is used [19]. Clearly, replacing BAC by some protocol based on the Diffie-Hellman key agreement [9] would protect against passive adversaries. To make it resistant to offline bruteforce attacks, one would need the notion of password-based authenticated key exchange [2,3,4].

Another issue in BAC is that e-passport could implement backdoors. When prompted by an (unauthorized reader) from a secret agency using some conventional way, the random number RND.ICC that is sent in clear by the IC chip could be selected so that the agency knowing a trapdoor would infer MRZ_info and run BAC without any visual contact to the passport.

Lazy BAC implementation could further make the IC chip select the final K.ICC so that the final seed is a constant and the the symmetric key is not session dependent.

*Active Authentication.* To bypass AA, one can try to do a relay attack (aka Mafia fraud [8]): one could try to authenticate to a reader and query a legitimate e-passport at the same time like a man-in-the-middle. This could be done with a fake reader and a fake e-passport communicating together through a private wireless link. This attack was detailed in [12].

One particularity of AA is that it is optional and only proves that the current chip is not a clone. This does not prevent the chip to be clones with the implementation of AA removed. Depending on the reader implementation, this can pass or not. Indeed, the cloned IC chip could announce itself as not being able to run AA. If the reader does not pay attention to the fact that SOD includes a DG15 (the AA public key that we cannot remove without altering the SOD signature), it will not bother the

chip with AA. For this reason, it is important to check if DG15 is present and to mandate the use of AA if present.

Another weakness of AA is in the protocol itself. Clearly, the AA protocol can be used to sign whatever the reader wants. It is not recommended to use this public key for any other use than just AA. Otherwise, bad interaction between this signature oracle and the extra application using the public key could be devastating. When the public key is only used for AA, the signature is not binding at all since it is commonly admitted that the chip signs whatever we submit to it. Nevertheless, the signature can be a proof that the IC chip has seen the challenge. We can elaborate on this property to add semantics in the challenge. Namely, we can use as a challenge a hash to all previously issued timestamps and to add the signature of it as a new timestamp. This would be a proof that the IC chip was used at a given time, and indeed an evidence that could be used in court. This is known as the *challenge semantics* attack [20].

*Leakage of digital evidence.* Another privacy threat is the leakage of a signature by government bodies of private information. Someone who considers his age, official name, or even real gender as the most private information would loose privacy. Clearly, showing his e-passport to anyone would leak a proof of it. His old passport used to contain the same information but in a non-transferable way. Although someone could make a copy of an old passport, the copy would not have been a proof itself since it is clearly easy to make a fake copy of a passport. With e-passports, this is no longer the case. A digital copy of the data groups and the SOD is also a proof by itself that can be shown to someone else.

For instance, it is commonly accepted to show a passport at the registration desk of an hotel. A clerk in the hotel could dump the LDS or an e-passport and later publish the picture DG2, name, birth date, and gender in DG1 together with the SOD which would prove that it is certified by government authorities.

Another place where we would have to show a passport would be in a duty free shop or in a supermarket to buy some vine. Clearly, employee from these shops could abuse the passive authentication concept by keeping digital evidence.

This transferability issue could be solved by using a non-transferable proof of signature knowledge [18].

*Abuse of automated identification.* Yet another privacy threat is the abuse of automated identification. Clearly, department stores having seen e-passports could collect biometrics together with profiles and do automated recognition. The digital picture in DG2 is not only a picture but also a high quality image that was optimized for automatic face recognition. Together with video surveillance, this could automatically identify a customer entering again in the shop and show his profile and last purchase. While being valuable for stores, this would violate the human right to remain anonymous in a crowd.

*Lazy identification.* One of the goal of the ICAO standard is to make identification automated. This also comes with the danger that security officers do a lazy job while trusting too much the technology. By doing such, clones of genuine IC chip (not implementing AA or with AA bypassed) in a fake passport of low quality would pass more easily. Since face recognition can easily have fake positives when two persons are alike, technology could become counterproductive.

*Denial of services.* People may try to grill IC chip by electromagnetic bombing. The e-passport holder may not even be aware that his chip is broken. The protocol at border control when the chip is no longer responding is not documented. Travelers may most likely be the victim of such DoS attack by spending several hours at the border control.

## 4 The EU Extended Access Control

Besides BAC, the ICAO standard lets better access control open as the *Extended Access Control* (EAC). Implementing and using EAC requires for the issuing country and the visiting country to have a bilateral agreement on that. Typically, the European Union is developing its own EAC to be used by members in the Schengen area. The first version is available in [20]. To make it simpler, we refer to it as *the* EAC, although there may be other EAC in development in other countries.

One objective of the EAC is to use more biometrics than a facial image and to treat them as sensitive data, while the facial image and MRZ would be considered as "less sensitive data". Following EAC, access to sensitive data would be protected by a stronger access control. At the same time, secure messaging would be protected by a key coming from a stronger key agreement.

The EAC essentially contains two new protocols: chip authentication and terminal authentication. To treat sensitive data, both of them must be used. For other purposes, chip authentication can be used alone. Actually, chip authentication could be used to replace AA and have a better session key at the same time with better security.

*Chip authentication.* Chip authentication consists of a Diffie-Hellman protocol [9] where the IC chip uses a static Diffie-Hellman public key (authenticated from SOD) and the reader uses an ephemeral one. The produced key is used to replace the secure messaging key. This way, the secure messaging channel is semi-authenticated in the sense that the IC chip is authenticated to the reader. It is further resistant to passive attacks.

*Terminal authentication.* Access control is strengthened by having a true reader authentication. This requires a new PKI for readers. We assume that countries will build a new PKI and have certificates for every authorized reader. Since revocation is quite harder (e-passport do not receive revocation lists), the validity period would be rather short: from 1 day to 1 month. Revocation would thus be based on expiration.

Terminal authentication works like AA: the terminal gives his certificate, the IC chip sends a random challenge, the terminal signs it together with its Diffie-Hellman ephemeral public key (which was used in the chip authentication), and the IC chip checks the signature. It is claimed in the specifications that unlike e-passports, terminals do not have privacy problems so the challenge semantics attack is pointless.

*Overall identification procedure.* In identification, the sequence of steps from the ICAO standard is extended. After facial recognition is made, the terminal and the IC chip can run chip authentication, then terminal authentication. Then, the terminal can load the fingerprint image, the iris image, and check whether it matches the holder.

## 5 Security and Privacy Issues in EAC

A few weaknesses on the EAC are already reported. Besides issues from the ICAO standard which are not resolved by EAC, we list here a few issues.

*Chip authentication.* Chip authentication "only" provides semi-forward secrecy. Namely, if the IC chip is not tamper proof and the fixed Diffie-Hellman secret key is corrupted, past communications can be decrypted. This contradicts the specifications which announces forward secrecy. Secondly, man-in-the-middle attacks would still be possible just like the attack against AA from [12].

*Terminal authentication.* As already admitted in the EAC, the revocation issue based on time is pretty weak since e-passports have no reliable clock. The best they can do is to maintain an increasing value of the last time value given by an authenticated terminal, but this will only protect frequent travelers. Occasional travelers can still be the victim of unauthorized access with an expired key.

If we now focus on an honest terminal with a cheating e-passport, the claim of not having privacy issues in terminals is a free claim. We could still imagine a journalist willing to show that he could pass the security control with a forged e-passport. The challenge semantics against the terminal could be used as a proof that he passed after being checked by some given employee who could then be threatened in his job.

*Leakage of sensitive data.* EAC protects more sensitive data from unauthorized access. However, some little information about it leaks before EAC is used. Namely, the SOD contains the hash of all data groups and can be read after BAC. This means that if we have a guess for a privacy sensitive data group, we can check it before EAC. Furthermore, if privacy sensitive data groups have little entropy, we can get them by bruteforce form their hashes. Finally, if we have a sketch for a data group, e.g. a fingerprint capture from the holder, depending on whether the mutual entropy with the template is high or not, we can reconstruct the original template from its hash.

To fix this, it would be safe to include an unused random number of high entropy in every data groups.

## 6 Conclusion

Although increasing security at border controls, e-passports create new security and privacy threats.

First of all, e-passports may be tracked due to basic RFID protocols. Shields should thus be used.

Second, BAC offers a pretty minimalist security. It does not complete its task of protecting against passive skimming. It should replaced by a better protocol.

Third, AA leads to challenge semantics attacks and should be replaced e.g. by the EAC chip authentication. Using it should be mandatory to protect against chip cloning.

Fourth, to avoid abuse of automated identification, some kind of terminal authentication (like the EAC one) should be used. This should even be done before passive authentication so that SOD would not leak in the open world. Ideally, passive authentication should be made with a proof of signature knowledge rather than by a signature exhibition.

Hopefully, this would keep a pretty good security while maintaining a reasonable level of privacy for people.

## References


1. G. Avoine, Ph. Oechslin. RFID Traceability: A Multilayer Problem. In *The 9th International Conference on Financial Cryptography (FC'05)*, Roseau, The Commonwealth of Dominica, Lecture Notes in Computer Science 3570, pp. 125–140, Springer-Verlag, 2005.
2. M. Bellare, D. Pointcheval, P. Rogaway. Authenticated Key Exchange Secure against Dictionary Attacks. In *Advances in Cryptology EUROCRYPT'00*, Brugge, Belgium, Lecture Notes in Computer Science 1807, pp. 139–155, Springer-Verlag, 2000.
3. S. M. Bellovin, M. Merritt. Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks. In *IEEE symposium on Research in Security and Privacy*, Oakland, California, USA, pp. IEEE Computer Society Press, 72–84, 1992.
4. V. Boyko, P. MacKenzie, S. Patel. Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman. In *Advances in Cryptology EUROCRYPT'00*, Brugge, Belgium, Lecture Notes in Computer Science 1807, pp. 156–171, Springer-Verlag, 2000.

5. D. Carluccio, K. Lemke-Rust, C. Paar, A.-R. Sadeghi. E-Passport: The Global Traceability or How to Feel Like an UPS Package. To appear in the proceedings of the RFID Security workshop 2006, LNCS.
6. G. Davida, Y. Desmedt. Passports and Visas Versus IDs. In *Advances in Cryptology EUROCRYPT'88*, Davos, Switzerland, Lecture Notes in Computer Science 330, pp. 183–188, Springer-Verlag, 1988.
7. G. Davida, Y. Desmedt. Passports and Visas Versus IDs. *Journal of Cryptology*, vol. 11, pp. 253–258, 1992.
8. Y. Desmedt. Major Security Problems with the Unforgeable (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them. In *The 6th Worldwide Congress on Computer and Communications Security and Protection (Securicom'88)*, Paris, France, pp. 147–149, SEDEP, 1988.
9. W. Diffie, M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, 1976.
10. J. Hall, M. Barbeau, E. Kranakis. Detecting Rogue Devices in Bluetooth Networks using Radio Frequency Fingerprinting. In *Proceedings of the Third IASTED International Conference on Communications and Computer Networks (CCN'06)*, Lima, Peru, pp. 108–113, IASTED/ACTA Press, 2006.
11. 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.
12. 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
13. 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.
14. 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.
15. 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.
16. 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
17. 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
18. J. Monnerat, S. Vaudenay, M. Vuagnoux. About Machine-Readable Travel Documents: Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication. Presented at the RFID Security Workshop 2007. To appear.
19. S. Rudich. The Use of Interaction in Public Cryptosystems. In *Advances in Cryptology CRYPTO'91*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 576, pp. 242–251, Springer-Verlag, 1992.
20. Technical Guidelines TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents — Extended Access Control (EAC). Version 1.01. Federal Ministry of the Interior. Bundesamt für Sicherheit in der Informationstechnik. 2006.
http://www.bsi.de/fachthem/epass/EACTR03110_v101.pdf