

The FIDIS Network of Excellence



The European Information Society (EIS) requires technologies which address trust and security yet also preserve the privacy of individuals. As the EIS develops, the increasingly digital representation of personal characteristics changes our ways of identifying individuals, and supplementary digital identities, so-called virtual identities, embodying concepts such as pseudonymity and anonymity, are being created for security, profit, convenience or even for fun. These new identities are feeding back into the world of social and business affairs, offering a mix of plural identities and challenging traditional notions of identity. At the same time, European states manage identities in very different ways. For example, in Germany holding an ID card is mandatory for every adult, while in the UK state-issued ID cards do not exist. [FIDIS objectives](#) are shaping the requirements for the future management of identity in the EIS and contributing to the technologies and infrastructures needed.

Budapest Declaration on Machine Readable Travel Documents (MRTDs)

- [Abstract](#)
- [Introduction](#)
- [Summary of Findings](#)
- [Recommendations for the Stakeholders in Europe](#)
- [Resources](#)
- [Footnotes](#)

Abstract

By failing to implement 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. In this declaration, researchers on Identity and Identity Management (supported by a unanimous move in the September 2006 Budapest meeting of the FIDIS “Future of Identity in the Information Society” Network of Excellence[1]) summarise findings from an analysis of MRTDs and recommend corrective measures which need to be adopted by stakeholders in governments and industry to ameliorate outstanding issues.

Introduction

Whilst still susceptible to traditional ID document abuse scenarios, new Machine Readable Travel Documents (MRTDs) offer numerous additional threats. From these we wish to stress that:

- In contrast to traditional ID documents, European MRTD data are remotely, transparently and non-interactively readable (from the perspective of the passport owner) from a distance of 2 to 10 meters[2]. This is compounded by access control which is susceptible to circumvention or

hacking (therefore risk of ubiquitous, unobserved authentication to MRTD data by authorised or unauthorised third parties, enabling tracking of people carrying a passport, for example when residing as a tourist in a foreign country)

- Use of biometric data stored on ID documents is exploitable by both the public and private sectors for additional purposes - a violation of European privacy principles. Moreover, biometrics themselves are based on probabilities, thus false positive and negative authentication is unavoidable and will potentially affect many European citizens every day.

Based on the international technical ICAO[3] standards defined in document 9303[4] and following Regulation EC 2252/2004[5] in European legislation, implementation of the European passport (epass) as an international MRTD began in 2005. This position paper is based on the analysis of the legal grounds for MRTDs, the technology involved and the implementation of data protection and security. This analysis has been undertaken by the FIDIS NoE and documented in the FIDIS Deliverable D3.6 "Study on ID Documents"[6]. The following material has also been considered for the formulation of this position paper:

- Protection Profiles for Biometric Verification Mechanisms and MRTDs including Basic Access Control (BAC)[7] certified by the German Federal Office for Information Security (BSI)
- Technical Guideline V1.0 for Extended Access Control (EAC) issued by the German Federal Office for Information Security (BSI) in August 2006[8].

Summary of Findings

No coherent, integrated security concept for MRTDs has been disclosed to either the public or interested experts. Publicly available documents such as the Protection Profiles and Technical Guidelines cover only parts of such a security concept[9]. BAC was presented originally as an effective access control solution, while more recently EAC has been presented as an enhanced version. However, both are simply insufficient (as access control for the user) in many situations.[10]

A number of theoretical and scientifically demonstrated threats and conceptual weaknesses of MRTDs have already been published. These are not, as yet, covered by Protection Profiles, technical guidelines and standards or existing implementations. Most significant among these are:

- Biometrics in MRTDs currently cannot be revoked and since biometric features of the users such as fingerprints and facial features cannot easily be changed, "stolen" biometrics can be abused for a long period of time
- Insufficient key management with BAC: The key to access data on the RFID tag is stored on the passport itself and can be read by humans and machine scanners. This means that anybody who has had physical access to the passport and e.g. made an optical copy, could store the key information and use it to access data on the RFID tag
- Eavesdropping of communication between RFID tag and reader and brute force attack on BAC using documented cryptographic weaknesses to discover data[11]
- Cloning of RFID tags in MRTDs[12]
- Abuse of the remote readability of RFID tags in passports, for e.g. person sensitive ignition of 'smart bombs'

The combination of these threats and weaknesses puts the security and privacy of European citizens at significant risk. This is especially true considering the geographically broad usage and long lifetime (up to ten years) of current MRTDs.

Recommendations for the Stakeholders in Europe

Based on these findings we have developed a number of recommendations for European stakeholders (politicians, industry and research) in the area of MRTDs:

1. Since MRTDs with inherent weaknesses have already been introduced and will inevitably be used in future, we recommend the following measures for immediate implementation to reduce the risk of security failure and identity theft. These recommendations include scenario-based back-up procedures and technologies which require an international level of development and agreement (i.e. ICAO):
 - a. Organisational implementation and enforcement of the purpose binding principle especially for biometrics used in MRTDs (where the defined purpose is authentication of

- international travellers). The use of MRTDs should not be extendable to authentication in the private sector.
- b. Citizens need to be informed of the risks inherent in owning new MRTDs and the corresponding security measures which can be undertaken by them (for example avoiding the release of the documents to private organisations such as hotels etc.)
 - c. Available yet unimplemented security measures such as Faraday cages should be integrated immediately into current MRTDs by the European member states.
 - d. Organisational procedures are necessary to cater for the failure of biometric authentication due to inherent biometric issues such as false rejection rates (FRR) and error to enrol.
 - e. Organisational and technical procedures are required to prevent abuse of personal data from MRTDs.
 - f. Organisational and technical procedures are necessary to deal with identity theft using data from MRTDs or complete MRTDs.
2. In the mid term (within the next three years) a new convincing and integrated security concept covering MRTDs and related systems needs to be developed and communicated. In particular, this must take into account:
- a. A definition of required security levels.
 - b. Protection of European citizens' personal data (including biometrics if still utilised).
 - c. Multilateral technical and organisational security aspects of the deployment of MRTDs considering different operators in different countries and the MRTD users (exemplary question: How can abuse of personal data by foreign countries be prevented?)
 - d. Risks and threats emerging from the combination of different technologies used in the context of MRTD such as RFID, biometrics, and security features of paper-based documents.
 - e. Based on the defined security levels and risk analysis, a complete re-evaluation and re-design of the technical solutions adopted for current MRTDs, especially RFID and biometrics, should be performed. It should be considered whether these technologies are actually necessary, or if technologies which are more secure and privacy-preserving (such as contact smartcards instead of contactless mechanisms) are sufficient. Ways in which the implementation of technologies utilised can be improved (e.g. for biometrics through the use of on-card matching and on-card sensors) should also be investigated.
 - f. The security concept should be publicly debated by security and privacy experts on a European level.
3. Technical and organisational measures developed need to be standardised (ICAO), implemented in the next generation of MRTDs, and audited world wide.

Resources

- (en) Budapest Declaration [[PDF-en](#)] [[URL](#)] [[Press Release \(en\)](#)]
- (de) Budapest Erklärung [[PDF-de](#)] [[URL](#)] [[Press Release \(de\)](#)]
- (fr) Déclaration de Budapest [[PDF-fr](#)] [[URL](#)]
- (se) Budapestdeklarationen [[PDF-se](#)] [[URL](#)] [[Press Release \(se\)](#)]

Footnotes

[1] FIDIS - "Future of Identity in the Information Society". See <http://www.fidis.net>

[2] ISO 14443 chips of the type used in MRTDs are optimised to work with the respective reader equipment in the area of 10 to 15 cm. However, eavesdropping the conversation between such passports and readers from longer distances (2-10 m) is possible (see Finke, T., Kelter, H., Radio Frequency Identification - Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, Bonn 2004. Download: www.bsi.de/fachthem/rfid/Abh_RFID.pdf) and has recently been demonstrated by Robroch with a Dutch passport (see Robroch, H., ePassport Privacy Attack, 2006, www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf), who also lists distances for reading and eavesdropping.

Some MRTD are equipped with additional shielding in their cover, e.g., US passports will contain a web of metal fibre embedded in the front cover. However, Mahaffey and Hering demonstrated that if a passport opens only half an inch — as may occur in a purse or backpack — it can reveal itself to a reader at least two feet away (see www.flexilis.com/epassport.php).

[3] ICAO = International Civil Aviation Organization, www.icao.int

[4] Information available via www.icao.int/MRTD/Home/Index.cfm

[5] See http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf

[6] Available at www.fidis.net/fidis-del/period-2-20052006/#c961

[7] Protection Profile BSI-PP-0016-2005 and BSI-PP-0017-2005, available via www.bsi.de/zertifiz/zert/report.htm

[8] Announced at www.bsi.bund.de/fachthem/epass/eac.htm

[9] For example, the Protection Profiles are only guidelines for security measures with respect to defined products (technical components) in the context of MRTDs; the degree and the quality of their implementation in existing MRTDs such as the epassport is not described in the text. Documentation of existing epassports with respect to the implementation of these Protection Profiles currently does not appear to be publicly available. Existing Technical Guidelines, e.g. the guideline on Extended Access Control (EAC) also only cover parts of the technical security.

[10] Extended Access Control (EAC) for example will be applied only to selected elements of the personal data stored on the epass (notably data categorised as especially sensitive such as biometric fingerprint data), while data such as the digital face picture and other personal data such as name, date of birth etc. are not covered. The use of EAC cannot be internationally enforced as EAC is not an international standard accepted by the ICAO. This means that in non-European countries only Basic Access Control (BAC) with a significantly lower security level will be used.

[11] The key strength may go down to 35 or even 28 bit if e.g. the passport numbers are dependent on other data in the passport (as it is the case e.g. in the Netherlands and in Germany). (See Beel, J., Gipp, B., ePass - der neue biometrische Reisepass, Shaker Verlag, Aachen 2005. Download of chapter 6 "Fazit": www.beel.org/epass/epass-kapitel6-fazit.pdf).

[12] See e.g. www.wired.com/news/technology/1,71521-0.html