Security Issues with RFID enabled Passports and Government issued eID Documents, an overview of risk scenarios and attack vectors

Lukas Grunwald
NeoCatena Networks Inc.
Pleasanton, CA 94588, USA
lukas@neocatena.com
http://www.neocatena.com

Blackhat Abu Dhabi - Emirates Palace 2010

Abstract

This paper is showing some risk of the use of ÏnsecureËRFID implementation on Passports and Government ID Documents for Automatic Immigration (E-Gates) as well how easy a identity could be stolen.

A overview of already existing electronic ID will be given, as well new work of the new German eID with Multi-Usage for Government, Legal as well private use for Parking-Meters, home Banking as well e-commerce.

1 MRTD Design

The electronic passport and the new mandatory eID for every citizen in Germany as well as every legal alien with permission to work or stay longer than 90 days, includes, in addition to the classical passport security measures, a smart card controller that communicates over an RFID interface that meets the ISO- 14443 standard.

1.1 Architecture

The architecture holds certain weak points, that are however only obvious to those with a detailed knowledge of the passport's underlying concepts and technologies. After an introduction to these basics, we will present potential risks from the perspective of an IT security expert. First of all, we look at the RFID chip's design: It uses a smart card controller of a type that is produced by Philips/NXP or Infineon. In most cases these are dual interface controllers, which means that they have a PIN interface (using the ISO 7816-XX standards) as well as an RFID interface. However, since travel documents are exposed to a lot of physical stress and have to last up to ten years the electronic passport's contact interface has been dropped in favor of the RFID ISO-14443 interface. The RFID reader has to be able to read the tag, as the RFID chip is often called, from a distance of less than 10 cm (about four inch).

1.2 Crypto Processor

Faster Encryption with Crypto Hardware: It is a small Computer After the card has been activated, its operating system is loaded and programs can be executed. These programs are written in Assembler, C or Java and run directly on the smart card after being translated into the processor's machine code. The RFID chips that are used for electronic passports additionally include acceleration hardware for cryptographic functions.

1.3 File structure

The up to 72 kByte of data stored on the chip inside the passport can be divided into two groups: Meta information files (EF.SOD and EF.COM) and data files (DG1 to DG20). EF.COM is a kind of index including information on which data groups exist on the tag. EF.SOD (security object data) includes the signed hash value, which is needed to verify its authenticity. The EF.COM, which defines what additional security functions are available inside the eID or ePassport, is not cryptographically signed. As a result, these additional security features (which are optional for the ePassport and to a certain extend for eIDs as well, when used as travel document) can just be stripped of clones.

The individual data groups include the following information: DG1 stores an electronic version of the machine readable zone (MRZ), the machine readable line that is printed on the passport's first page. This data group holds information such as the document number, its issuer, its duration of validity as well as the owner's name and birth date. This file is mandatory. DG2 holds the owner's picture, which should also be printed on the document itself. It is stored in CBEFF (Common Biometric Encoding File Format, ISO 19785). This format, which has been pushed by the industry lobby, creates a (unnecessary) meta layer, which includes the definition of the biometric format used in the document. The following two data groups, DG3 and DG4, are optional files, used for other biometric data such as iris scans and

finger prints. Over the time the ICAO introduced the following optional data groups to store more and more information on the eID as well MRTDs.

DG	Stored data
DG1	Machine readable zone (MRZ)
DG2	Biometric data: photo
DG3	Biometric data: fingerprints
DG4	Biometric data: iris
DG5	Photo as printed in passport
DG6	Reserved for future use
DG7	Signature as appears in passport
DG8	Security features: data features
DG9	Security features: structure features
DG10	Security features: material features
DG11	Personal details (address, phone)
DG12	Document details (date of issue, issued by)
DG13	Optional details (anything)
DG14	EAC Data
DG15	Active authentication public key
DG16	Persons to notify

2 The Reinvention of the Wheel

The description language for data structures in ASN.1 follows the same idea as XML: If offers a description language (Lex) that is used to define the document format. This allows creating a parser and an automated data generator by providing a processor with the language description. As a consequence it should be possible to easily create complex protocol parsers with already existing and tested libraries and quickly verify data correctness. However, this only works if the ASN.1 standard is observed, which the MRTD does not. Those responsible for planning the electronic travel documents designed entirely new tags based on the ICAO standard and therefore reinventing the wheel. Because of that, instead of an automatically generated one a handwritten parser is necessary. The data is, however, encoded according to the X.690 standard.

2.1 Quite not X.690

The X.690 standard describes data encoding in TLV (type-length-value). The basic encoding rules (BER) laid out in this standard describe how certain syntax notations in ASN.1 are mapped to the TLV structure. Again those responsible for the new electronic passport chose a different way: Instead of describing the passport's data structures in ASN.1 they just kept the TLV format which is actually fully defined by the BER. Thus, they defined tags that according to the BER could never exist. Because of that, there is no way to describe the passport's data using ASN.1 since a BER compatible ASN.1 encoder would create a different TLV-encoding. As a consequence also in this case a parser has to be built by hand or exceptions have to be inserted into standard libraries. In summary, all passport checks require purpose-built readers and cannot use standardized ones.

3 Basic Cryptographic Security

Cryptography first comes into play when performing the so called basic access control (BAC). However, one can't help but think that this concept offers only little security. In order to prevent passer-bys from reading the electronic passport, an önly optional p̈rotection of the transmission line (the radio interface) is intended. The data of all data groups is stored in plain text. In order to allow for a tamper-proof connection, this connection has to be encrypted. The key used for the initiation of this connection is generated from the MRZ. How this works in detail is specified in the ICAO standard. The reader has to (optically) read the page with the picture and the printed MRZ. The software then uses this data to generate a key that is used to set up an encrypted connection between the reader and the RFID controller. This way the reader signs on to the passport. If the key is incorrect, the passport cannot be read. The BAC encryption is optional; it is left to the passport issuer to decide whether to use it or not. If a passport supports it, the data cannot be read in plain text.

3.1 Upgrated eID Security

With the eID it gets more insecure to read the official part of the eID since a CAN (Card Access Number) is printed on this card. With this Card Access Number or the MRZ the content of the eID can be read. Basic Access Control used 3DES but only with a very limited choice of symbols for possible keys this results in a low entropy key potentially susceptible to brute-force attacks. For this reason the German government introduced PACE (Password Authenticated Connection Establishment), which helps increasing entropy to establish a secure channel between the RFID chip and the eID / MRTD terminal. But one wonders how good the best and academically proved cryptographic algorithms are, when the key or access password is printed on top of the eID.

3.2 Know or guess

So, in order to read a passport the owner's name (spelled correctly), the birthday and the document number are required. However, this data, which is printed in the second line of the MRZ, is by no means secret. Not only the passport's owner but also many hotels or banks who occasionally store passport numbers for security reasons (for example when withdrawing money) may have knowledge of this data. All other required information can be found in static or non-personal data. Thus also unauthorized people can generate a key.

3.3 Terminal Certificates

For the eID a Terminal Certificate is needed - but with thousands of mobile readers within the police force, administration, social security and potentially many other sites, local and central, it seems only a matter of time until secret keys would leak and grant full access to the eID. Next problem: Since according to the ISO 14443 standard every tag has to have a unique chip ID, it would be possible to track the movement of passports and hence their owners without a BAC procedure. In order to prevent this, the ICAO standard intends to use random data which is regenerated every time the chip is initialized for reading instead of the ISO 14443 ID. Again entropy is low and it has to be investigated in how far this procedure can provide truly random data. If the random number's range is too small, it is possible to draw conclusions as to the common origin.

4 Extended Access Control

The so called Extended Access Control is supposed to restrict access to the data groups DG3 and DG4 by encrypting the data objects (DG3 and DG4 are not used in the already issued electronic passports of the Federal Republic of Germany). For decryption a public key infrastructure (PKI) has to be established on a global basis including all participating countries. Certificates expire after a period of time and it should only be possible to read data from DG3 and DG4 using a valid certificate. However, it is still unclear how the Certificate Revocation List (CRL) listing invalid certificates or their serial numbers will be handled and where it will be stored. As long as a lost root certificate cannot be recalled, it can be used by computer criminals to electronically forge data groups.

4.1 Solved Vulnerabilities

These vulnerabilities do no longer exist with the eID. The German Federal Office for Information Security resolved many of the ICAO pitfalls and the eID benefits from a much more secure concept and design but still a legacy of certain MRTD design mistakes remains. In order to prevent the manipulation of DG data, a hash value is computed over every data group. A master hash value is then computed over the sum of all hash values and signed with the certificate of the issuing country. The reader holds a list of the public keys of all participating countries. Using these it can validate the included data after reading the electronic passport's structure and computing the appropriate hash values. This signed hash value is then stored on the chip in the EF.SOD sector.

5 Vulnerabilities in the Concept

In order to successfully check the hash data, the signature has to be read which involves intensive format parsing. To do this, the inspection system first reads unchecked data, which is then parsed by the newly created ICAO formats. The whole system's complexity and the fact that existing, already audited libraries cannot be used make programming errors more than likely. The inability to program syntactically correct parsers and to properly handle formats has in recent years been one of the most common sources for software vulnerabilities, not the actual cryptographic procedures.

ICAO's complex muddle of formats causes several weak spots:

- Many formats that are hard to implement; data is first read unsecured and has to be picked apart by a jumble of standards and proprietary procedures in order to be validated.
- The key used for Basic Access Control is in no way connected with the MRZ, which is stored in DG1. It is thus possible to plant data into the system by using another MRZ. The inspection system has to compare the printed MRZ with the one provided by DG1; but only after parsing the data. This again provides opportunities to attack the system.
- If the data for the BAC is known it is possible to read the passport data at any time and store it on another dual-interface card, which also observes the ICAO standard. From the perspective of an ISO 14443 reader or an automatic inspection system, that does not validate the other (optical) security features, those plain tags look just like a regular electronic passport. This vulnerability has been demonstrated by us first at the Blackhat 2006 conference. A manual and optical check by a customs official will hopefully still lead to a refusal of the passport.
- If a country's private key is lost or (very unlikely) cracked, there is no way of recalling it. Instead the passports of all citizens would have to be collected and replaced, which would hardly be possible in reality.

6 The Future of MRTD

It is questionable whether the electronic ID documents will prove to be of much use to their new owners. When inspecting a passport, an otherwise closed system accepts data from a not trustworthy 72 Kbyte memory unit with micro controller there could just as well be any software but the ICAO layout running on the chip. The eID could embed malicious code to actively attack the inspection system. Would a customs official let an unknown person connect a USB stick to his or her PC?

Most certainly not, but this is exactly what happens with the electronic passport: Its data is initially read without any verification. Only after passing the data through several non-standard compliant hand-coded parsers can the reader validate the data.

The programmers of the German reference system ”Golden Reader Tool” (GRT) report that the implementation of the electronic passport API was a complex and difficult task. In general this rather increases the vulnerability to attacks. Maybe a team of IT security and data protection experts should have taken a look at the system before it was launched. The way it is implemented now, the golden rule KISS K̈eep it simple, stupidḧas been sunk in a sea of lobbyism, featurisms and national interests. This article does not at all regard the quality of biometric data which introduces its very own set of security issues with respect to wrong acceptance and refusal rates, as well as the impossibility to recover from a once compromised feature. The electronic ID’s future remains precarious.

References

[1] Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Version 2.03 `http://www.bsi.de`, (2010).

[2] Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit; Version 1.0 `http://www.bsi.de`, (2009).

[3] Metasploit - Penetration Testing Resources `http://www.metasploit.com`, (2010).

[4] RFDUMP, A rfid audit software by Boris Wolf and Lukas Grunwald `http://www.rfdump.org`, (2010).

[5] New attacks against RFID-Systems, Lukas Grunwald `http://www.blackhat.com`, (2006).

[6] RFID and Smart-Labels: Myth, Technology and Attacks `http://www.blackhat.com`, (2004).