

dn

**Der elektronische Personalausweis
Mehr oder weniger Sicherheit ?**

Systems

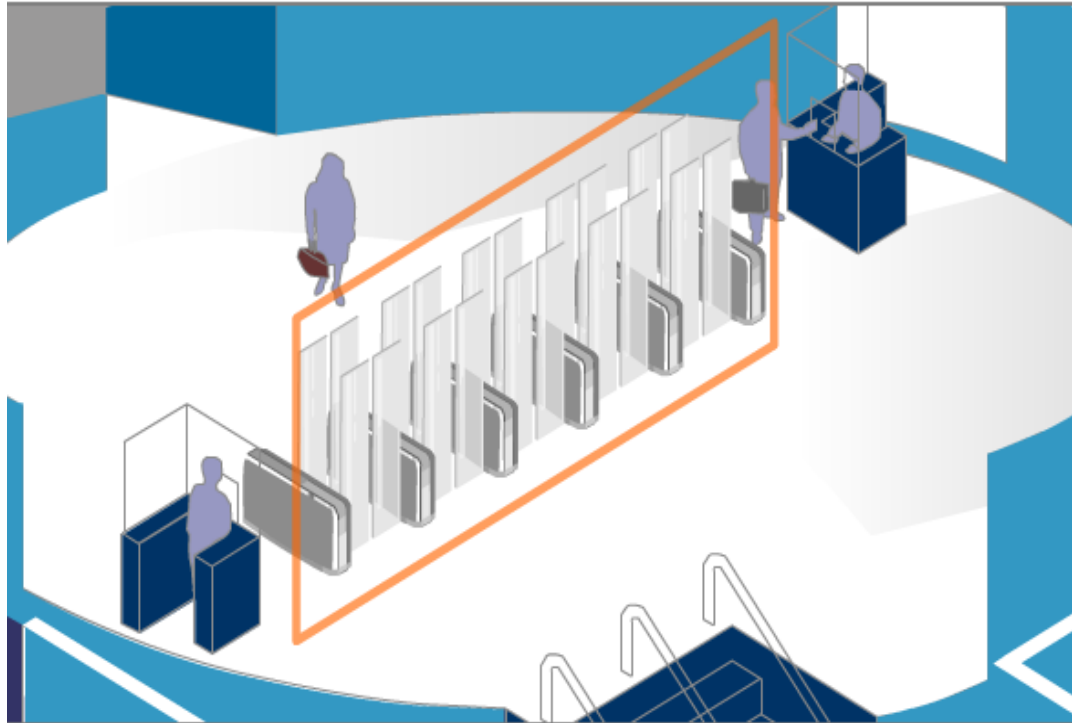
Lukas Grunwald

DN-Systems GmbH Germany

CeBIT 2010- Heise Forum

2010 Hannover

The Government's Dream



Multi biometric, double gates, anti-tailgating, lightly-supervised (to maintain non-automated entry channels)

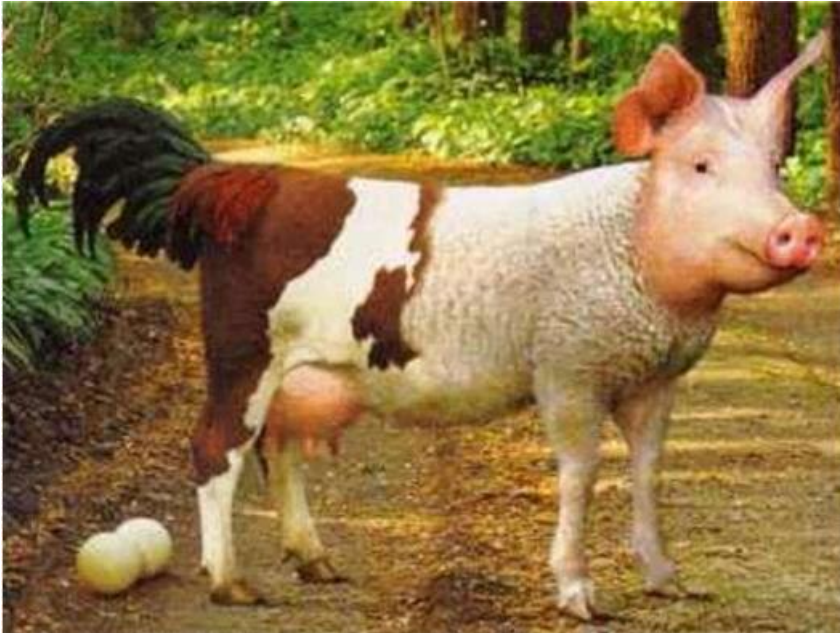
The Industry's Solution

- Government first asked Security Print Shops
 - These are general and global print shops
 - Extensive know-how in secure printing
 - No know-how in IT security / cryptography
 - Never done an IT security project
- Security Print Shops asked Smart Card Industry
 - Focus on selling their products
 - Advocates multi-purpose use

Industry Ideas for the eDocuments

- Multi-purpose use
- Identical design for national ID cards
- Use for electronic banking
- eGovernment
- Electronic signature
- Email encryption
- ID and travel / Passport
- Electronic payment

Design Goals



- Use of cryptography / PKI
- Heavy use of biometrics
- 100% security against counterfeiting
- Improve facilitation
 - Minimize time spent on legitimate travelers
 - Segmentation of low-, high-risk travelers
 - Minimize immigration time for traveler

Design Approach

- Setting up a standards group at the ICAO
- Stuffed with printing experts
- Some crypto experts
 - Only worked on algorithm level
- No one knows about implementation
- Driven by RFID manufactures
- No one looked at risks / design goals (KISS)



Problems with Patents

- To store biometric data, typically a HASH is generated and stored (for fast comparison)
- Most of these HASHES are patented
- ICAO stores pictures of facial image
 - JPEG or JPEG2000
- Same with fingerprints
- Compromises don't work with security



eID from Germany



- RFID tag embedded
- Produced by the Bundesdruckerei GmbH
- No shield, readable even when in pocket

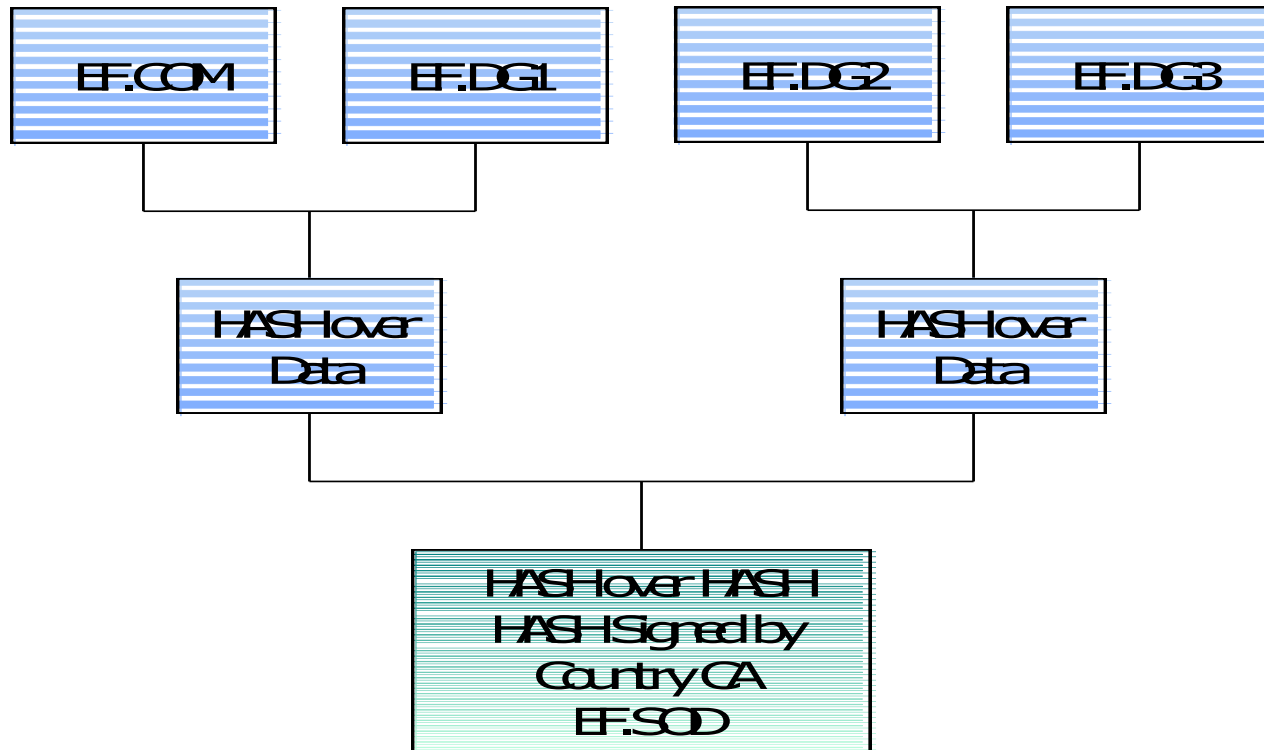
MRTD Security Features

- Random UID for each activation
 - Normally all ISO 14443 transponders have a fixed unique serial number
 - The UID is used for anti-collision
 - Prevent tracking of owner without access control
 - Problem: ICAO MRTD specs don't require unique serial number
 - Only some countries will generate random serial numbers

Non-traceable chip characteristics

- In 2008 a Radboud / Lausitz University team demonstrated that it's possible to determine where a passport chip is from without knowing the key required for reading it.
- The team fingerprinted error messages of passport chips from different countries.
- The resulting lookup table allows an attacker to determine where a chip is from.

Signed Data



LDS a deep technical view

The screenshot displays a hierarchical tree structure on the left and a hex dump on the right. The tree structure represents LDAP data with various object identifiers and sequences. The hex dump shows the corresponding binary data in hexadecimal and ASCII format.

Tree Structure:

- EF_SOD
 - FCP=6F1680020C1C8201018302011D88011D8A01058C03030000
 - FCI [APPLICATION 15] IMPLICIT SEQUENCE
 - 778204913082048D06092A864886F70D010702A082047E3082047A020103310B300906052B0E03021A050030540606678
 - [APPLICATION 23] IMPLICIT SEQUENCE
 - SEQUENCE
 - OBJECT IDENTIFIER = { 1 2 840 113549 1 7 2 }
 - [CONTEXT 0] IMPLICIT SEQUENCE
 - SEQUENCE
 - INTEGER 03
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 1 3 14 3 2 26 }
 - NULL
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 23 136 1 1 1 }
 - [CONTEXT 0] IMPLICIT SEQUENCE
 - OCTET-STRING 3046020100300906052B0E03021A0500303630190201010414F0840CBDB5B7
 - [CONTEXT 0] IMPLICIT SEQUENCE
 - SEQUENCE
 - SEQUENCE
 - [CONTEXT 0] IMPLICIT SEQUENCE
 - INTEGER 02
 - INTEGER 00EC
 - SEQUENCE
 - OBJECT IDENTIFIER = { 1 2 840 10045 4 1 }
 - NULL
 - SEQUENCE
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 6 }
 - PRINTABLE-STRING "DE"
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 10 }
 - UTF8-STRING "bund"
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 11 }
 - UTF8-STRING "bsi"
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 5 }
 - PRINTABLE-STRING "001"

Hex Dump:

```

02 02 02 .....
5C70 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5C80 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5C90 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5CA0 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5CB0 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5CC0 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5CD0 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5CE0 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5CF0 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D00 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D10 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D20 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D30 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D40 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D50 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D60 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D70 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D80 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5D90 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5DA0 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
5DB0 02 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 .....
  
```

LDS a deep technical view

The image displays a network protocol analyzer's view of an LDAP Search (LDS) packet. The left pane shows a hierarchical tree structure of the packet's contents, and the right pane shows the raw data in hexadecimal and ASCII.

Tree Structure (Left Pane):

- BIT-STRING 00304402204A54CE98EF703B797F014CB2B2082E17F3ACA55D82C1580C87B1F5E3F56D2CBB0220246186AAD21
 - SET
 - SEQUENCE
 - INTEGER 01
 - SEQUENCE
 - SEQUENCE
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 6 }
 - PRINTABLE-STRING "DE"
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 10 }
 - UTF8-STRING "bund"
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 11 }
 - UTF8-STRING "bsi"
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 5 }
 - PRINTABLE-STRING "001"
 - SET
 - SEQUENCE
 - OBJECT IDENTIFIER = { 2 5 4 3 }
 - UTF8-STRING "csca-germany"
 - INTEGER 00EC
 - SEQUENCE
 - OBJECT IDENTIFIER = { 1 3 14 3 2 26 }
 - NULL
 - [CONTEXT 0] IMPLICIT SEQUENCE
 - SEQUENCE
 - OBJECT IDENTIFIER = { 1 2 840 113549 1 9 3 }
 - SET
 - OBJECT IDENTIFIER = { 2 23 136 1 1 1 }
 - SEQUENCE
 - OBJECT IDENTIFIER = { 1 2 840 113549 1 9 4 }
 - SET
 - OCTET-STRING 5AF331495DF14E6581C59164F7185F05A4A06C1C
 - SEQUENCE
 - OBJECT IDENTIFIER = { 1 2 840 10045 4 1 }
 - NULL
 - OCTET-STRING 303D021D00ADBA2D31468185BCBE6A0D0C4D028FF63DADDA5B320D30AAC959B241021C3D74498F47D5BE

1927 spare bytes

Raw Data (Right Pane):

```

DE 7C 37 79 EB DD F6 FB
A5 05 E*040,|7yeY00W.
1DD0 49 C9 B5 54 57 3B
10 DF 26 83 3F B4 B7 76
C2 B7 IEµTW;.B&.?'·vÁ.
1DE0 3C AD F8 FE 83 9E
A4 30 CD C9 F6 29 54 6F
DF A7 <-øp..x0ÍÉó)ToBS
1DF0 91 5D 3D B6 1B 4A
87 13 E3 F8 70 40 A9 FO
E5 FB .]=µ.J..ãøp@øðãú
1E00 0E B6 C2 AA 65 F7
C6 31 10 F4 F4 1E B6 FO
8B 3F .µÁ*e+EL.óó.µð.¿
1E10 48 93 B6 20 F8 4F
0C FD 2D F1 95 05 F2 21
97 B2 H.µ ø0.ý-ñ..ò!.*
1E20 C5 E1 48 9F 68 43
D4 FO 2F C6 D4 OD AD A1
8B D9 ÁÁH.hC0ð/È0.-;Ú
1E30 51 87 D8 D4 F9 1D
DE A2 8F F6 31 71 1E 27
1D E1 Q.Ø0ù.P<.ø1q.'.á
1E40 32 8A AF 9B 1E 9E
DC 5D 71 40 98 D1 2D 49
5D F3 2.~...Ú]q@.Ñ-I]ó
1E50 D6 C8 66 01 C7 10
8F A6 AC 72 6D F4 90 0A
46 A3 ÖÈf.Ç...!-rmó..F&
1E60 78 6A 5E 38 9D E4
B5 9B 32 38 28 B3 50 7D
0C AE xj^8.äµ.28('P).ø
1E70 01 DD 9D EA DF 42
2A 19 A2 AF 51 42 71 F5
B1 C6 .Ý.êBB*.c~QBqô±E
1E80 A4 2A E2 94 F8 6A
5B FB EC 0A D1 F2 F6 CB
40 C5 *ª.øj[ùí.ÑòøÈ@Á
1E90 DA F8 C8 A9 55 BB
77 F3 OF F5 2E 11 08 47
02 44 ÚøÈ@U»wó.ö...G.D
1EA0 73 01 79 AA BB 45
76 63 F3 46 33 C4 ED 2A
AB A9 s.y*»EvcóF3Ái*«ø
1EB0 CA 6B 55 81 08 88
  
```

Basic Access Control (BAC)

- In 2005 Marc Witteman presented that document number of Dutch passports were predictable, allowing an attacker to guess / crack the key required for reading the chip.
- There is software on the internet that tries all known passport keys within a given range, thus implementing one of Witteman's attacks.
- Using online flight booking sites, flight coupons and other public information it's possible to significantly reduce the number of possible keys.
 - Note that in some early biometric passports BAC wasn't used at all, allowing attacker to read the chip's content without providing a key.

<http://sys-security.com/category/rfid/>

<http://sys-security.com/category/rfid/>

<http://www.dice.ucl.ac.be/crypto/passport/index.html>

Passive Authentication (PA)

- In 2006 DN-Systems demonstrated that it is trivial to copy passport data from a passport chip into a standard ISO 14443 JCOP smartcard using a standard contact-less card interface and a simple file transfer tool.
- My early Biometric ePass was used for this and did not change the data held on the copied chip to keep its cryptographic signature valid.
- In 2008 Jeroen van Beek demonstrated that not all passport inspection systems check the cryptographic signature of a passport chips.
- For his demonstration Van Beek altered chip information and signed it using his own document signing key of a non-existing country.
- Only 5 out of 60+ countries are using this central database.

<http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>

<http://freeworld.thc.org/thc-epassport/>

<http://dexlab.nl/downloads.html/>

Active Authentication (AA)

- Marc Witteman presented that the secret Active Authentication key can be retrieved using power analysis.
- This allows an attacker to clone passport chips that use the optional Active Authentication anti-cloning mechanism.

Removal of AA

- In 2008 Jeroen van Beek demonstrated that optional security mechanisms can be disabled by removing their presence from the passport index file. This allows an attacker to remove - amongst others - anti-cloning mechanisms (Active Authentication).
- Note that supplement 7 features vulnerable examples in the same document that - when implemented - result in a vulnerable inspection process.

<http://www.blackhat.com/presentations/bh-europe-09/VanBeek/BlackHat-Europe-2009-VanBeek-ePassports-Mobile-slides.pdf>

<http://www2.icao.int/en/MRTD/Downloads/Supplements%20to%20Doc%209303/Supplement%20to%20ICA0%20Doc%209303%20-%20Release%207.pdf#page=35>

Extended Access Control (EAC)



- In 2007 DN-Systems presented an attack that can make EAC-enabled passport chips unusable.
- We stated that if an EAC-key - required for reading fingerprints and updating certificates - is stolen or compromised, an attacker can upload a false certificate with an issue date far in the future.
- The affected chips block read access until the future date is reached.

Inspection Systems

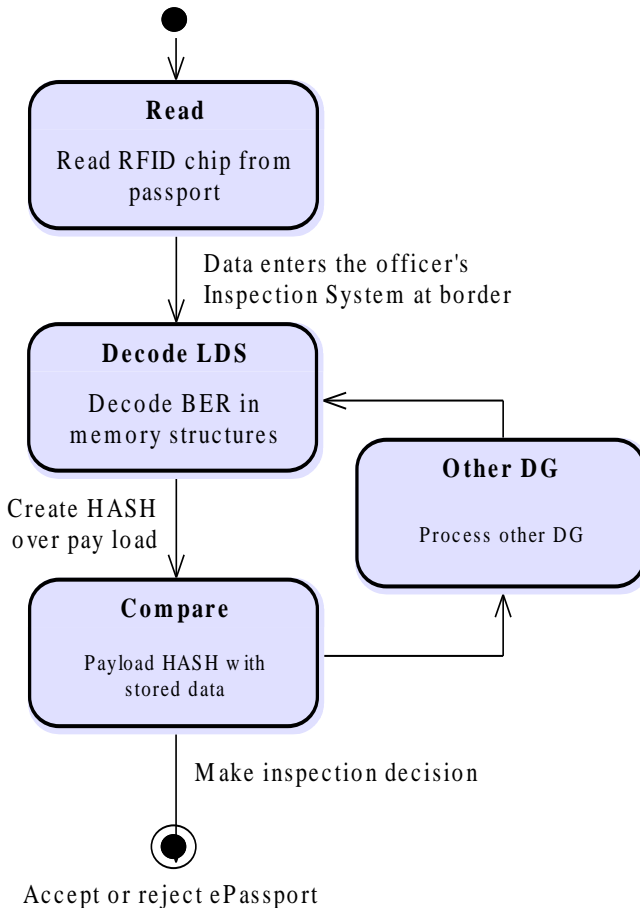
- Inspection systems should be evaluated
- Off-the-shelf PCs are too complex to be formally validated for correctness
- MRTD uses JPEG2000
- JPEG2000 is very complicated
 - Easy to exploit
 - For example, see CVE number CVE-2006-4391
 - Metasploit and other toolkits make it easy

A Vendor's Design of an Inspection System

- Uses “off-the-shelf” PC’s
- RFID-Reader is “Designed for Windows XP”
- No security improvement of the software
- Just like inserting a USB stick containing unknown data into the inspection system



Problem With The Procedure



- First, read, data from the RFID chip
- Then, parse the structures
- Decode the payload
- Finally, verify the document cryptographically

Biometric Data

- Data should be reduced to hashes only
- But fingerprints will be stored as pictures
- Reverse-engineering of fingerprints possible with MRTD data
- Contrary to any best practice in IT security

Chaos of Standards

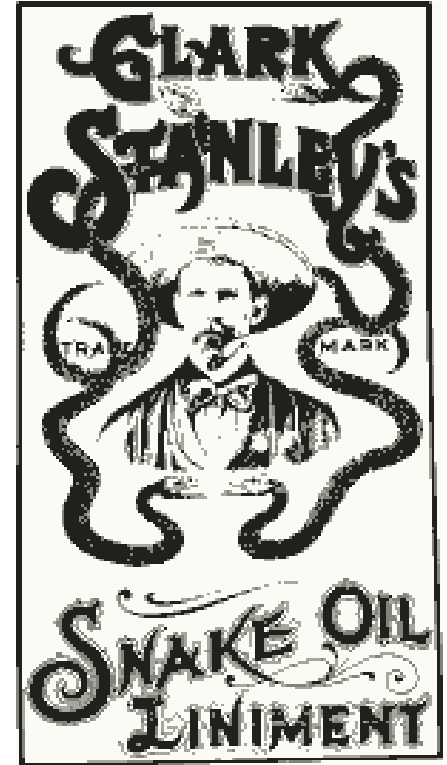
- TLV and ASN.1 not correctly implemented
- Redundant meta formats for biometric data
- If signing key is lost, the whole country is doomed
- First, the data must be parsed, then it can be verified
- Design was made by politicians and not by IT security experts
- It is possible to manipulate data

Why Cloning of eIDs?

- The normal tags are read-only
- Data could be retrieved from an issued passport
- Deactivation of issued passport (microwave oven)
- Cloned tag behaves like an “official” eID
- Cloned tag could be extended with exploits
- Exploit could attack inspection system, backend or databases

Snake Oil Warning

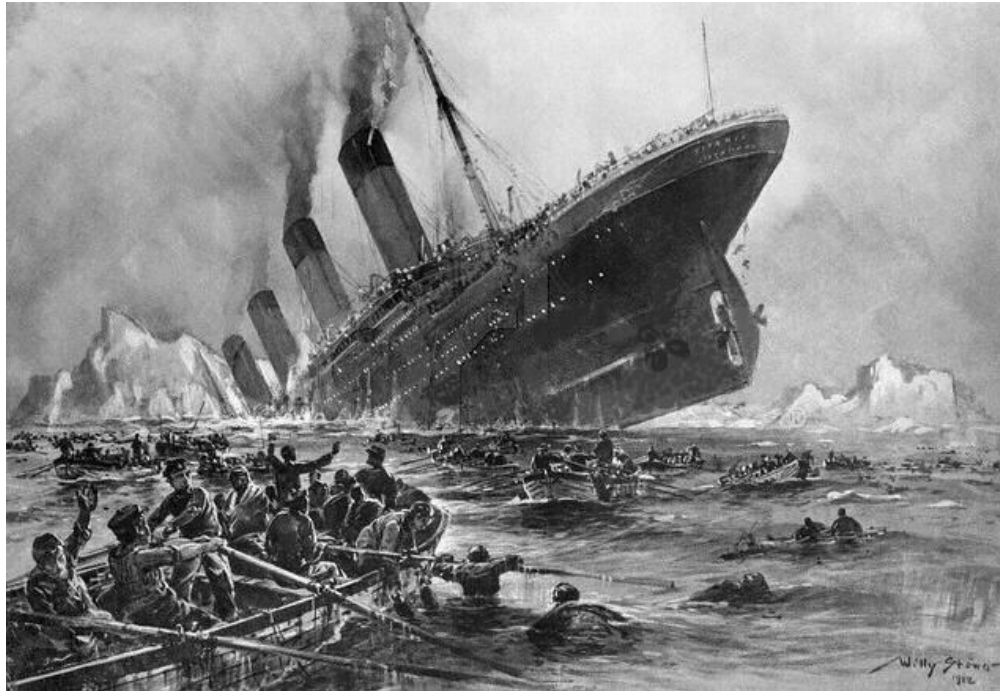
- “Trust us, we - the experts - know what we're doing”
- “We removed the standards from the ICAO website, now we are safe”
- “Grunwald used the primary purpose of the passport: he read it - there is no security risk”
- “The RFID chip will be protected by the security features of the printed paper in the passport”



More Quotes

- After a short presentation of some security issues at the “Security Document World 2007” in London I got this comment from a responsible person at the ICAO:
- “It’s right that these security flaws could harm an IT system, but we have to keep in mind, the ePassport is a security document and has nothing to do with IT systems”

Thank you, keep in mind ...



High-tech ≠ High-security