

# ePassports reloaded goes mobile



Jeroen van Beek  
BlackHat Europe 2009, Amsterdam




# Where will we go today?

- Technology overview
- Attacks
  - Demos!
- Impact
- Awareness
- EAC
- Solutions
- Questions



# Technology overview

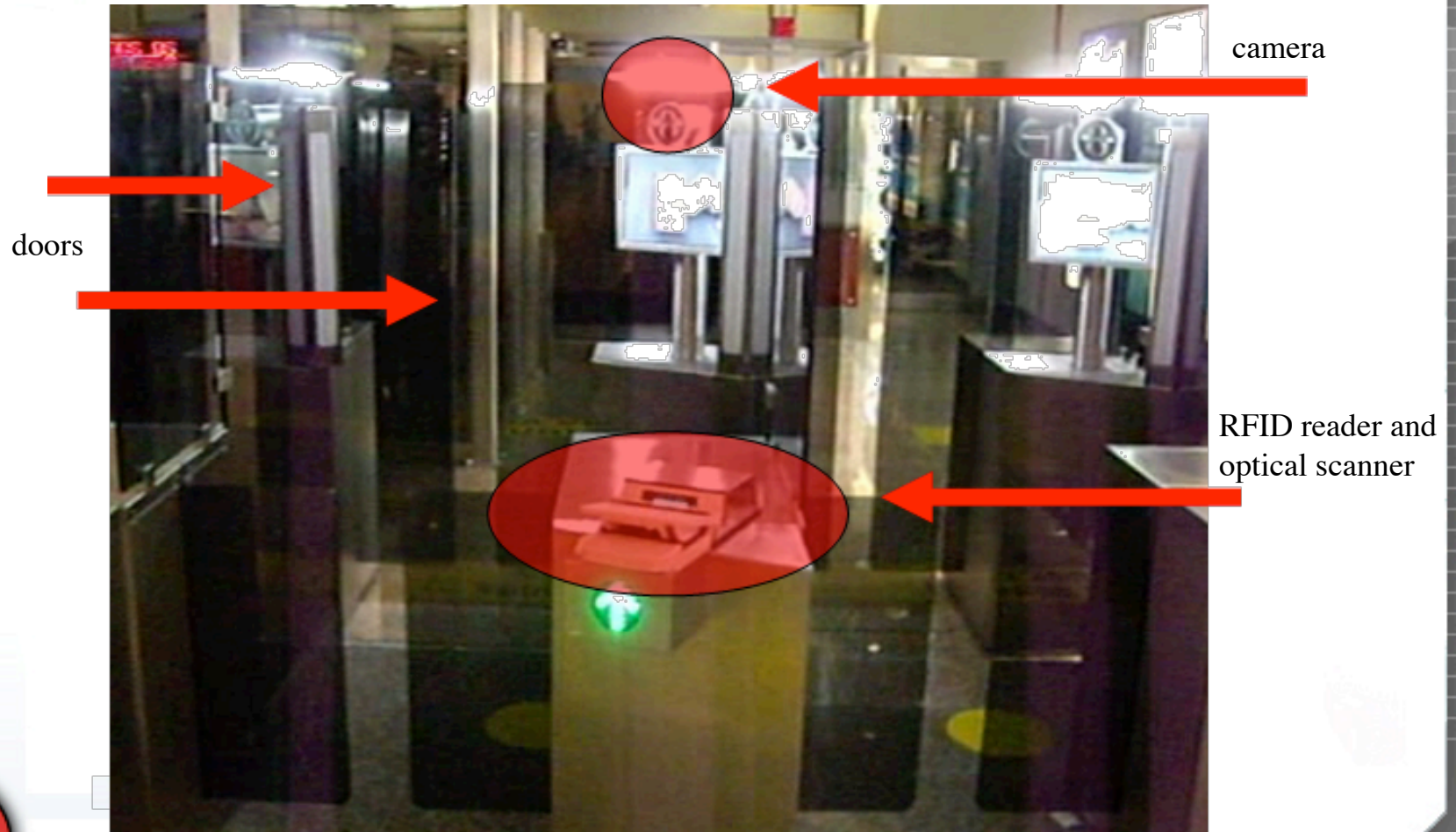
- An ePassport contains a chip
- The chip contains data about the passport holder
- Based on a standard by the International Civil Aviation Organization (ICAO) 
- **Chip content is accessible using a wireless interface (RFID)**
- ePassports are enrolled on a global scale
  - 60(+) countries at this time
- Not widely used for real-life applications (yet)
  - Some test setups seen in the field



# Technology overview, ct.

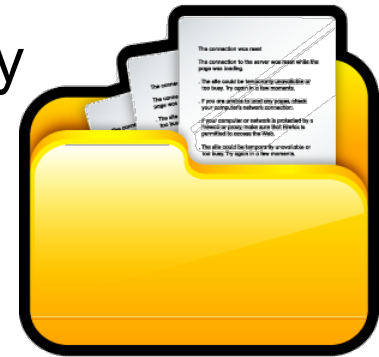


# Technology overview, ct.



# Technology overview, ct.

- Chip contains files:
  - Data Groups (DG) [1-16]
    - DG1: personal information, mandatory
    - DG2: picture, mandatory
    - Rest: optional (at this time)
      - DG15: anti-cloning crypto
      - Starting 28 June 2009 also fingerprints in the EU
  - Security object EF.SOD, mandatory
  - Index EF.COM, mandatory



# Question

- Can we pass border control with a fake chip?



You are here: [Home](#) > [News](#) > [News Topics](#) > [How about that?](#)

## Grandmother flies to Canary Islands on her husband's passport

A grandmother flew to the Canary Islands using her husband's passport by accident.

Last Updated: 12:50AM BST 25 Jul 2008

Andrea Cole picked up the wrong passport when leaving her Cardiff home for the week-long holiday with her mother, and did not realise her mistake until minutes before their flight was due to leave.

The mother-of-three had already passed through two sets of checks at Cardiff International Airport - and was then allowed through immigration at Fuerteventura without the error being spotted.

Mrs Cole, a self-employed computer technician, said: "I just couldn't believe what had happened. You would expect people to double check in this day and age."

 [Email this article](#)

 [Print this article](#)

 [Share this article](#)

### Related Content

**The Sophie Butler report: Losing a passport**



# Path of attack: step 1

- Document should *look* genuine
  - For men and machine
    - Oldsk3wl craftsmanship
    - **Just buy a blank document...**
  - Hide the fake chip
    - Disable the original chip
      - Microwave oven
      - Hammer
  - **Demo included later on!**





Page last updated at 09:37 GMT, Tuesday, 29 July 2008 10:37 UK

✉ E-mail this to a friend

🖨️ Printable version

## 3,000 passports and visas stolen

**Greater Manchester Police has launched an investigation into the theft of 3,000 blank passports and visas.**

The documents were in a van which was targeted on 28 July.

The Foreign Office admitted a serious breach of security over the loss of the passports and visa stickers, which were being sent to embassies overseas.

A former Scotland Yard fraud officer said the passports may be worth £1,700 each and could be used to set up bank accounts or get employment.

The theft is the latest in a series of security breaches but Labour's deputy leader, Harriet Harman, has denied



The Foreign Office has admitted a serious breach of security

“ I don't think that it necessarily shows a sloppy attitude ”

### SEE ALSO

- ▶ Previous cases of missing data  
15 Jun 08 | UK
- ▶ MoD admits another laptop stolen  
20 Jul 08 | UK
- ▶ MoD admits loss of secret files  
18 Jul 08 | UK

### RELATED INTERNET LINKS

- ▶ Foreign and Commonwealth Office
- ▶ Identity and Passport Service

The BBC is not responsible for the content of external internet sites

### TOP UK STORIES

- ▶ Mortgage loans reach 'record low'
- ▶ Six held over honeymoon killing
- ▶ Sikh girl wins bangle law battle

The passport service said the stolen documents could not be used by thieves because of their hi-tech embedded chip security features.

## Medewerker Schiphol steelt blanco paspoorten

ANP

gepubliceerd op 09 april 2009 09:25, bijgewerkt op 09:27

[Printversie](#) 

[Deel dit artikel](#) 

SCHIPHOL - Een 36-jarige platformmedewerker op Schiphol wordt verdacht van diefstal van blanco Nederlandse paspoorten van de luchthaven. Dat maakte de Koninklijke Marechaussee, die de man aanhield, donderdag bekend.

De marechaussee begon het onderzoek naar hem nadat onderhoudsmedewerkers van een woningbouwvereniging in de meterkast van de oude huis van de verdachte de paspoorten hadden aangetroffen.

### **Creditkaarten, hotelvouchers**

De marechaussee arresteerde de man op Schiphol. In zijn auto en huidige woning werden onder meer creditkaarten, hotelvouchers en een navigatiesysteem aangetroffen. De marechaussee denkt dat hij deze spullen ook heeft gestolen uit postzendingen.

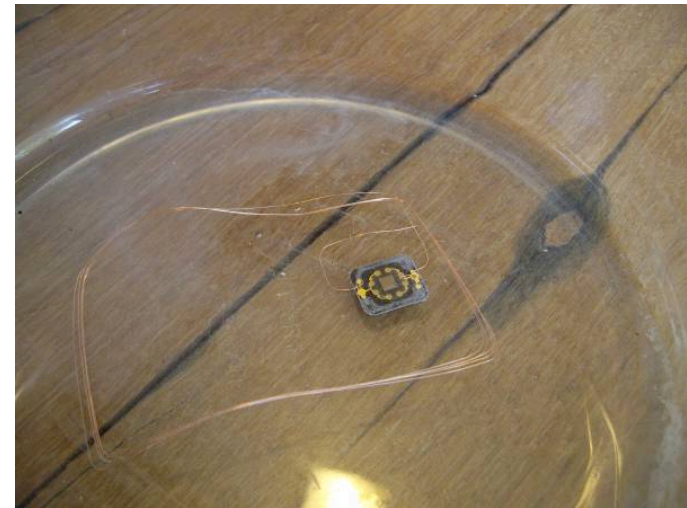
De paspoorten zaten vorig jaar in een diplomatieke postzending naar Vancouver in Canada.

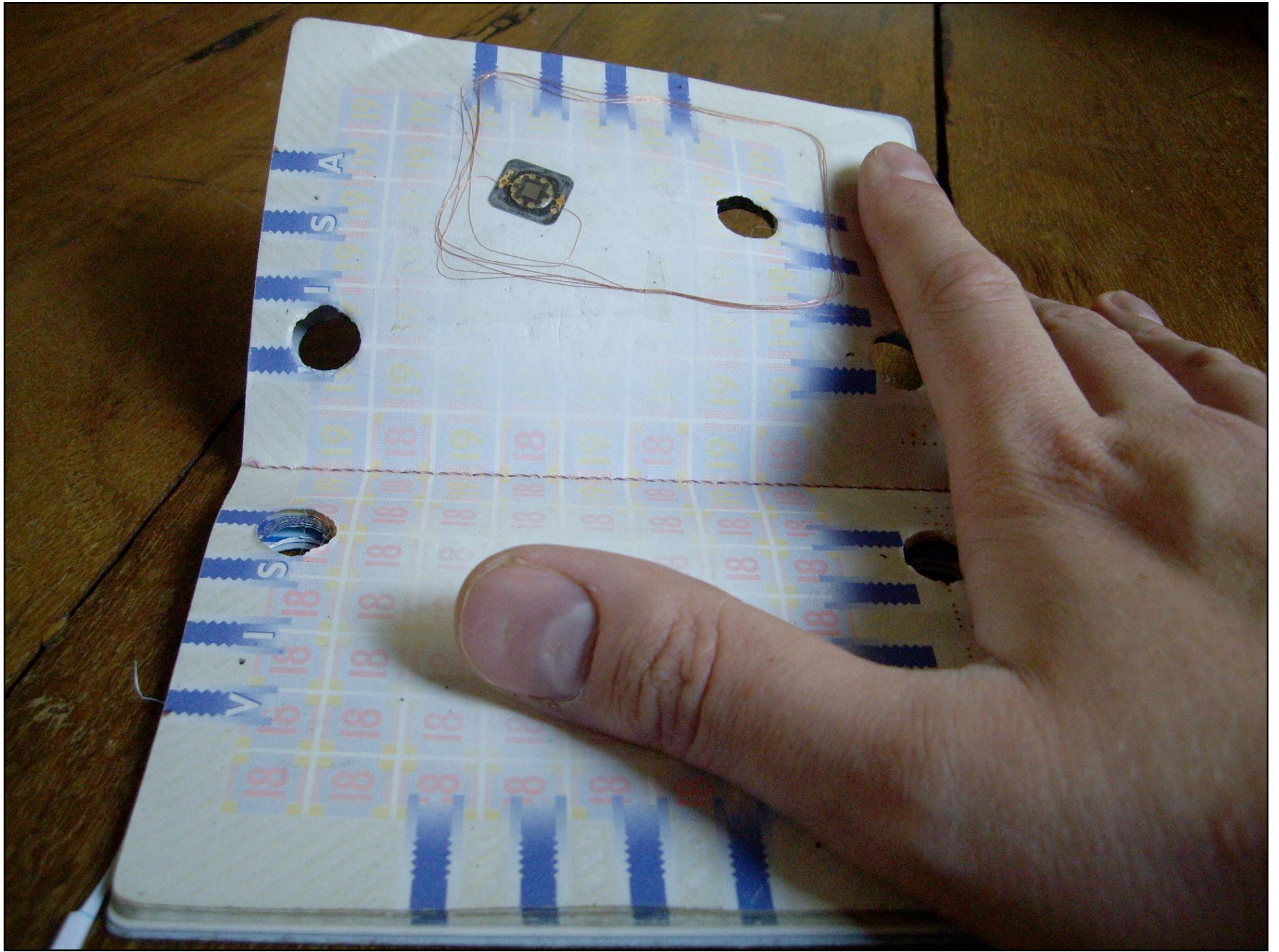
“Employee Amsterdam Airport steals blank passports”  
Passports were part of diplomatic mail.

# Path of attack step 1, ct.



+





## Path of attack step 2a

- Clone the original chip content
  - 100% copy
    - A copied PKI signature is still valid
  - Use the copy in a fake document
    - Your own twin brother / sister!
  - Dress to impress
    - Wig
    - Moustache
    - Etc.



HOME > NEWS > NEWS TOPICS > POLITICS > LAW AND ORDER

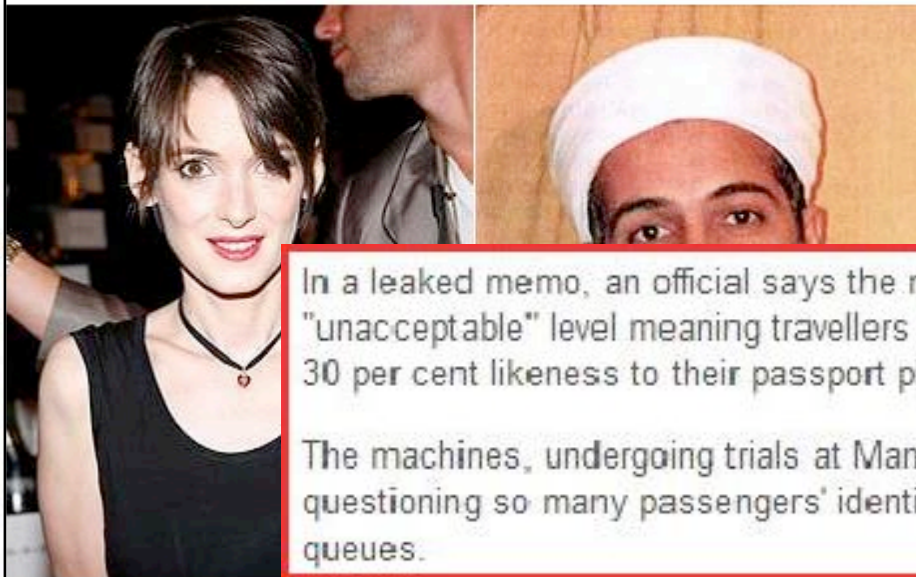
# Airport face scanners 'cannot tell the difference between Osama bin Laden and Winona Ryder'

Airport face scanners designed to verify travellers' identity against their passport photographs are working at such a low level that they would be unable to tell the difference between Osama bin Laden and the actress Winona Ryder, it has been claimed.

By Duncan Gardham, Security Correspondent  
Last Updated: 9:10PM BST 05 Apr 2009

- T Text Size + -
- ✉ Email this article
- 🖨 Print this article
- ▶ Share this article
- Digg

Law and order 



In a leaked memo, an official says the machines have been recalibrated to an "unacceptable" level meaning travellers whose faces are shown to have only a 30 per cent likeness to their passport photographs can pass through.

The machines, undergoing trials at Manchester airport, have apparently been questioning so many passengers' identities that they were creating huge queues.

Osama bin Laden and Winona Ryder: airport face scanners reportedly cannot tell the difference Photo: GETTY; EPA

In a leaked memo, an official says the machines have been recalibrated to an "unacceptable" level meaning travellers whose faces are shown to have only a

NEWS VIDEO: UK POLITICS LATEST ▶



00:00 00:19

▶ ✉ email 🔗 get link 🔄 get code 🗄 🗣



Nato protests in Strasbourg

Brown addresses G20 gathering

Lord Mandelson on G20 talks

ie!  
geselecteerd!

2009 om 18:34

ogenblikken geleden  
aar en als mogelijke  
p AQUOS LCD TV

Indien u bent uitgekozen, klik dan hier.  
<http://www.geselecteerde-winnaar.nl/>

## Path of attack step 2a, ct.

- Clone the original chip content
  - Active Authentication should stop you
    - Detect emulators using asymmetric crypto
    - Seen in The Netherlands, Belgium, Latvia, Finland, ...
  - Optional(!) mechanism
    - Used in approximately 20% of the implementations
    - Not used in the US, UK, Japan, ...
      - » These countries implicitly accept lookalike fraud







## Path of attack step 2a, ct.

- Attacking Active Authentication
  - Not writing the public key (DG15) doesn't work
  - What about manipulating index EF.COM?
    - If file DG15 is not there you can't check it...
  - Demo!



# Path of attack step 2a, ct.

- Remove files from index EF.COM

```
0 1 2 3 4 5 6 7 8 9 a b c d e f
00000000h: 60 15 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 ; \_...0107_6.0400
00000010h: 30 30 5C 03 61 75 6E ; 00\.au
```



# bytes - 1  
# tags  
DG1 (required MRZ info)  
DG2 (required picture)  
DG15 (optional active authentication)

```
0 1 2 3 4 5 6 7 8 9 a b c d e f
00000000h: 60 14 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 ; \_...0107_6.0400
00000010h: 30 30 5C 02 61 75 ; 00\.au
```

- This downgrade attack can also be used to strip future optional files including fingerprints
- Issue is reported in [supplement 7 of Doc 9303](#)
  - R1-p1\_v2\_sIV\_0006: an adequate workaround is “rejected”
  - Same document (p19) & other ICAO examples feature vulnerable examples



# Path of attack step 2b

- Clone content creation process
  - Real passport number
  - Real name
  - Other picture



# Path of attack step 2b

- Clone content creation process
  - Passive Authentication should stop you
  - Security object (SOD) stores:
    - A hash of all original files
    - Public key of signing certificate
    - Digital signature over itself
  - Changes can be detected

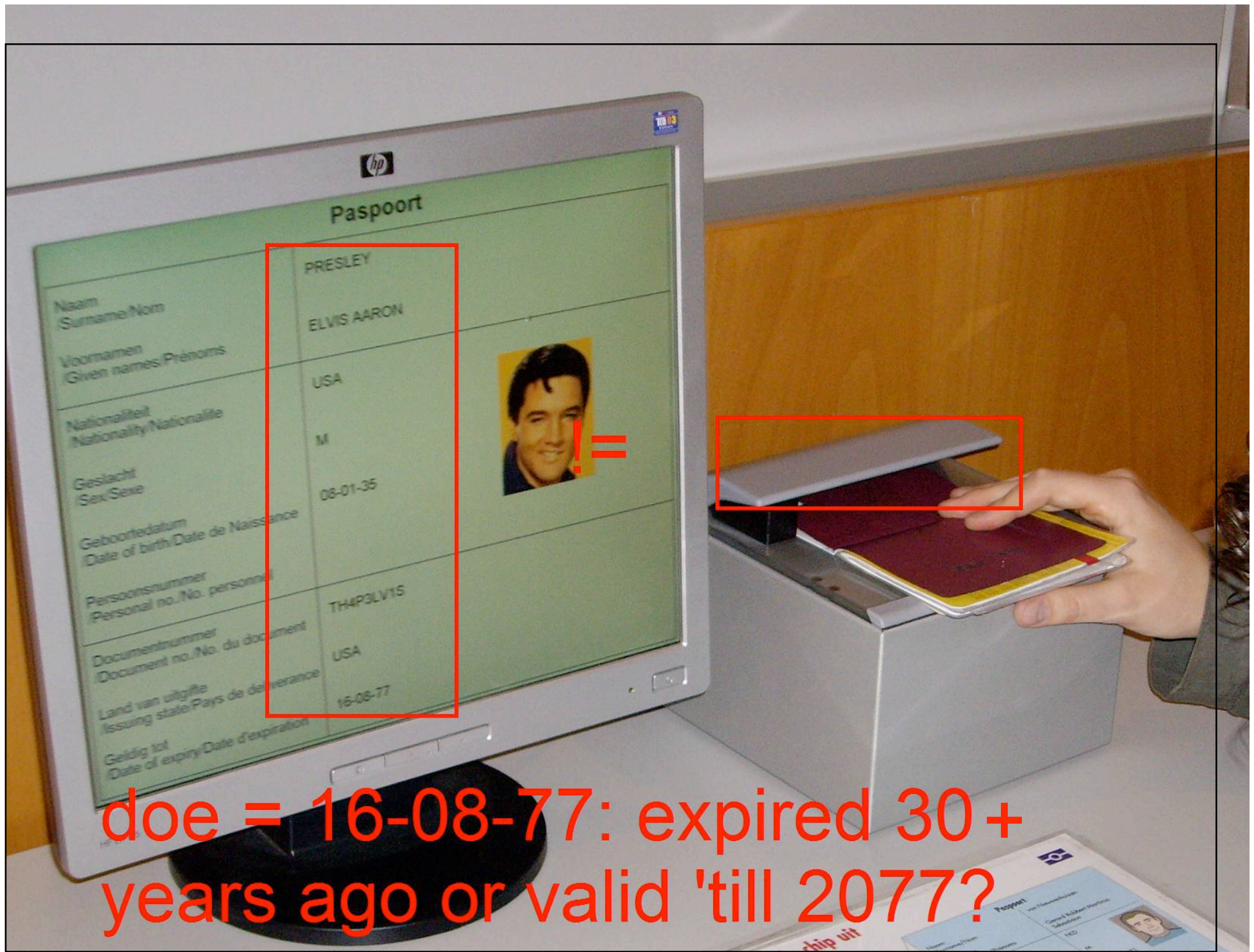




# Path of attack step 2b, ct.

- Attacking Passive Authentication
  - Country keys are self-signed
  - Authorized public keys of all countries should be available for inspection systems to check trustworthiness
  - ICAO Public Key Directory ([PKD](#)) should facilitate this
    - Chips enrolled in 60(+) countries
    - ICAO, April 2006: PKD membership should be “*necessary...and not optional*”
    - ICAO, May 2008: “*The ICAO PKD has grown to nine participants*”
    - Fall-back mechanism: “*distributed by strictly secure diplomatic means*”
      - Manual process: higher risk of (un)intended human errors
      - What about e.g. key exchange Israel ↔ Iran?
  - Create your own self-signed certificate and sign altered data
    - Start your own country!
    - Thanks to Peter Gutmann and his [CryptLib](#) library
    - [Demo!](#)



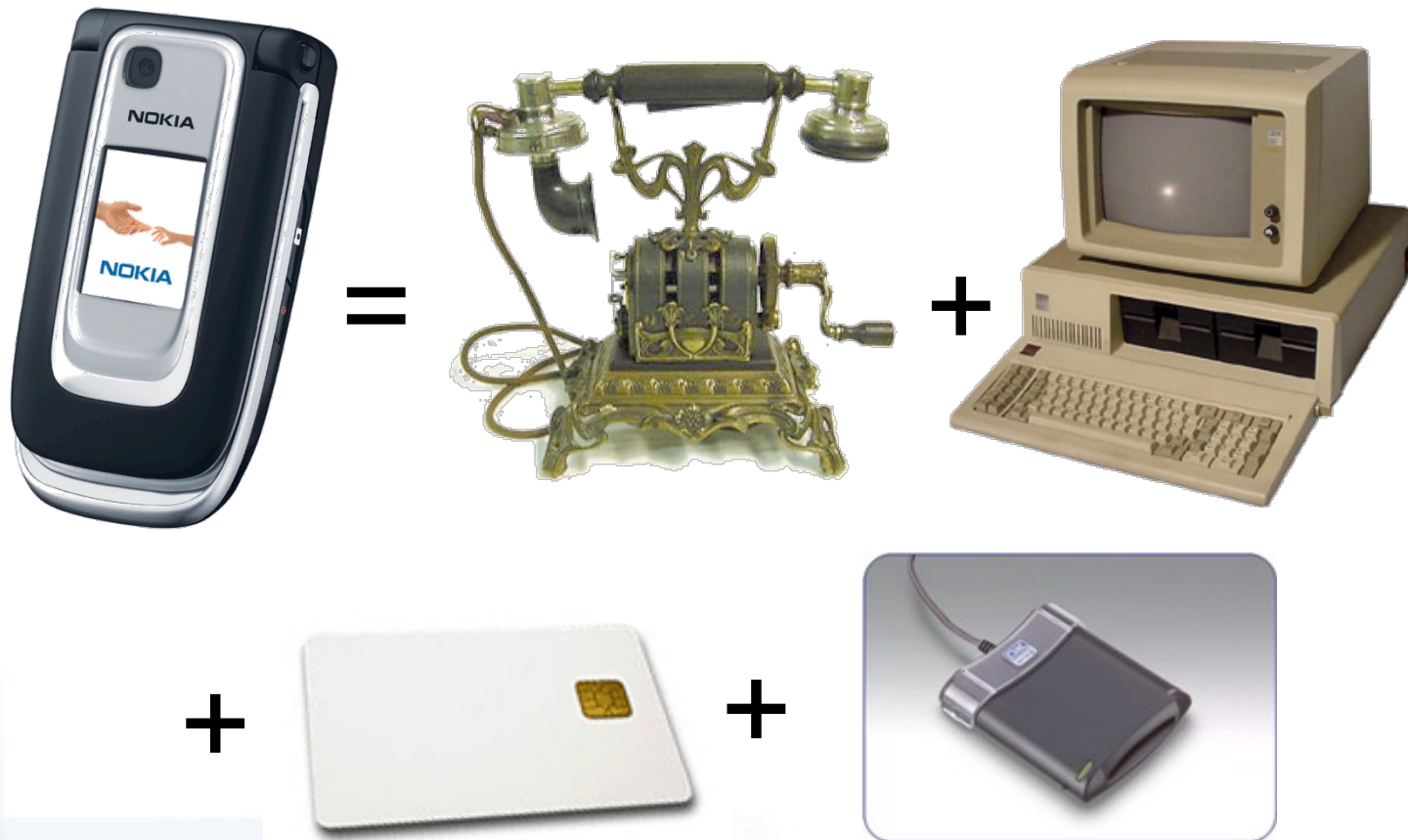


doe = 16-08-77: expired 30+ years ago or valid 'till 2077?





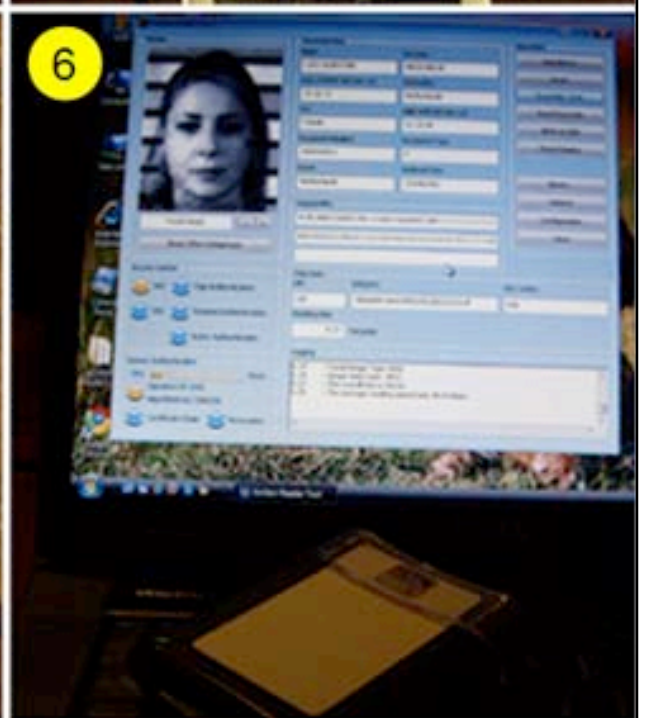
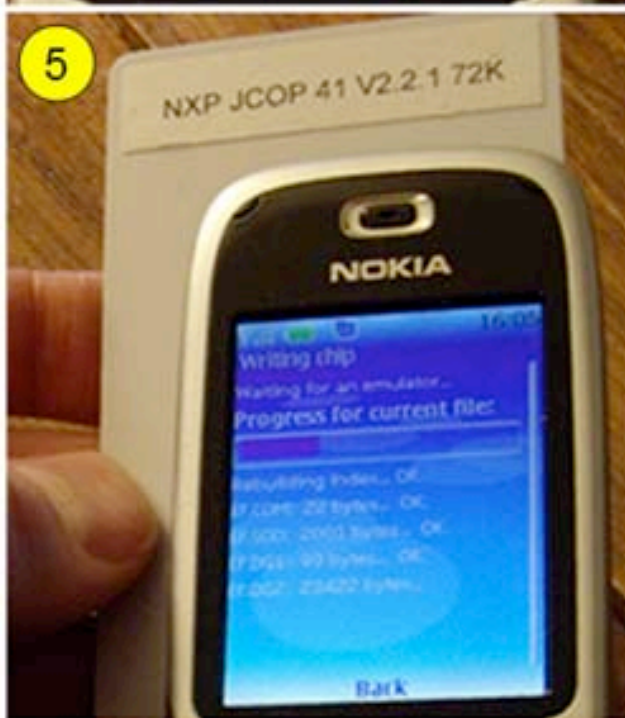
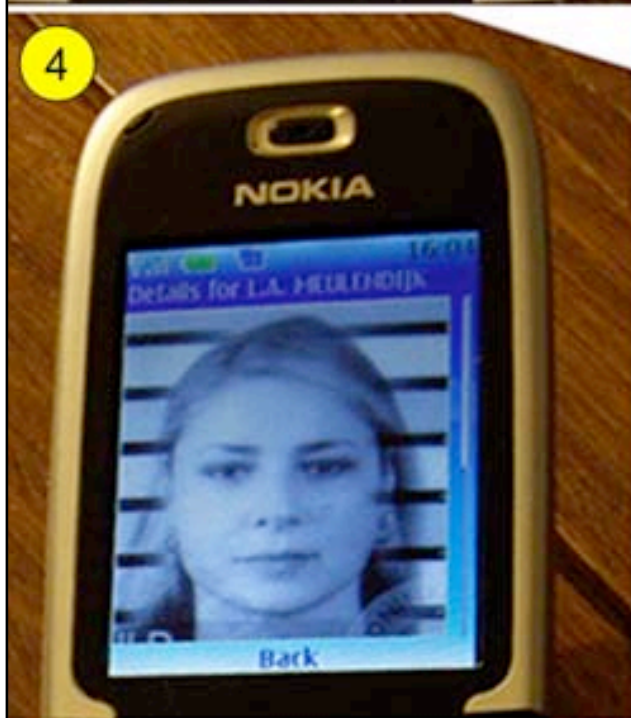
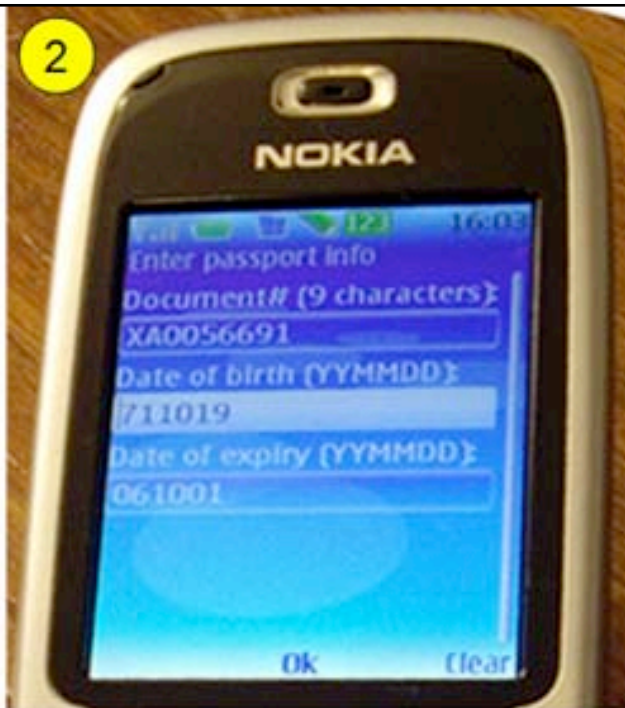
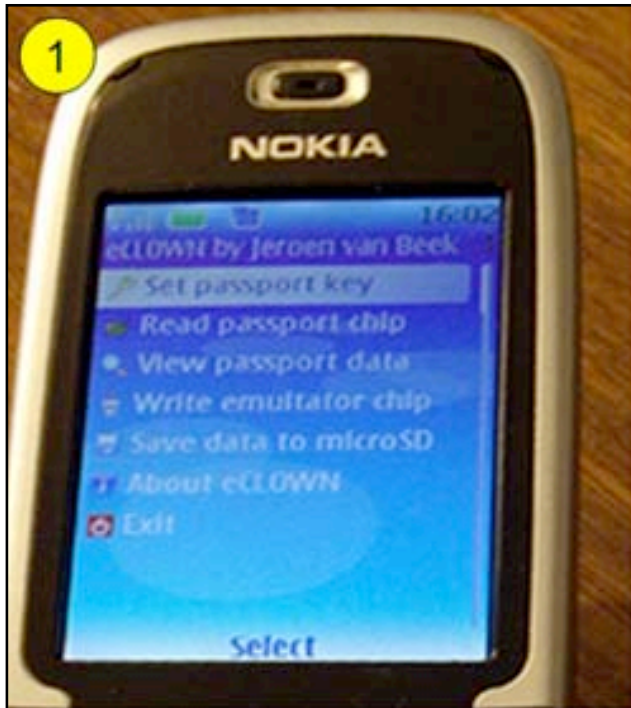
# Clone with your phone



# Clone with your phone, ct.

- Modern Near Field Communication (NFC) phones include:
  - Phone functionality
    - Not interesting for now :)
  - Computing power
    - Run your own applications including all kinds of crypto etc.
  - A “secure element” (Nokia)
    - JCOP v4.1 compatible including Mifare emulation mode
    - You can [unlock](#) the secure element to run your own applications
    - **Backup your passport chip content to your phone**
  - An RFID interface
    - Send and receive APDUs
    - **Read ePassports chips**
    - **Write ePassport emulator chips**
- That’s exactly what we need to clone ePassports!
  - [eCLOWN](#): clone an ePassport with your phone!
  - Thanks to Collin R. Mulliner for bringing this technology to my attention
- **Demo!**





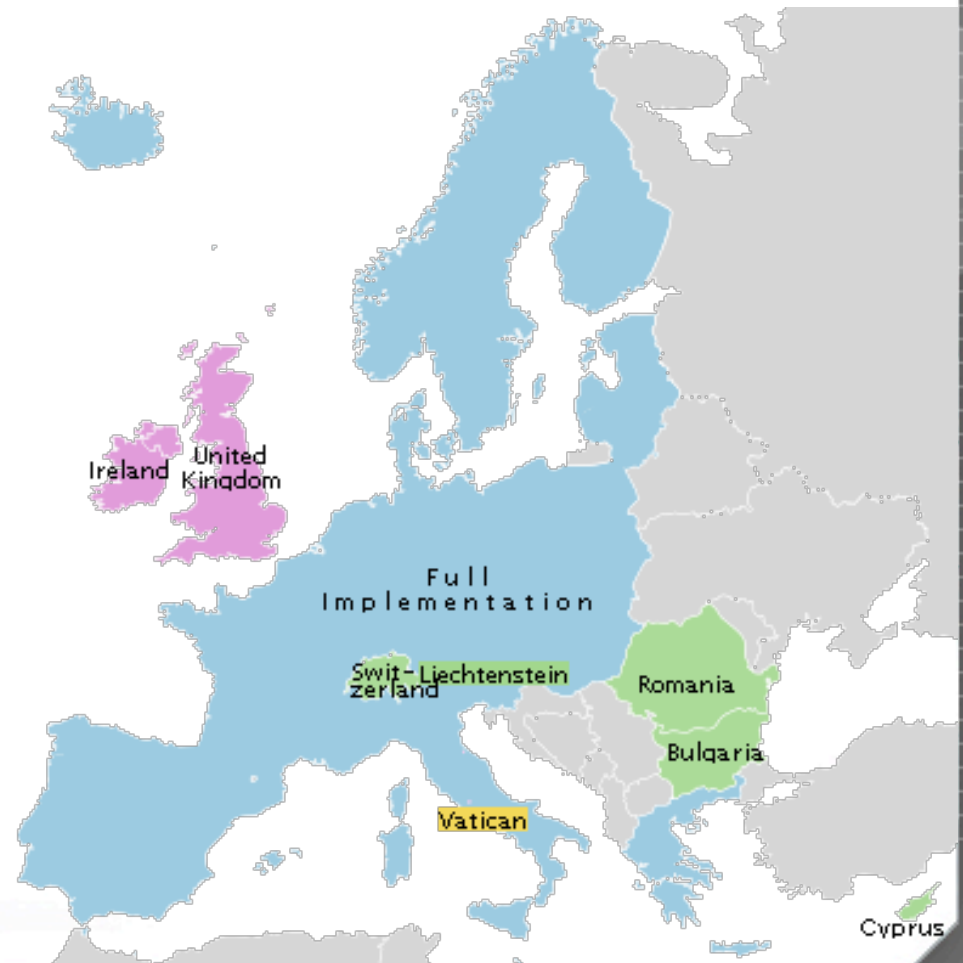
# Man In The Middle

- MITM support in Adam Laurie's latest RFID tools
  - One card emulator, one reader, a transparent link
  - Including socket support
    - Connect to a reader on the other side of the world
  - Get it from [rfidiot.org/RFIDIOT-0.1y-beta.tgz](http://rfidiot.org/RFIDIOT-0.1y-beta.tgz)
  - Demo!



# Impact

- Passport-free travel zone EU
- Are all implementations 100% secure?



- Police and judicial cooperation only
- Set to implement later
- Expressed interest



# Awareness



- Chip functionality is documented
  - ICAO Doc 9303
  - Annual interoperability test events
- Inspection system functionality is not documented
  - No standard
  - No known test events
  - Everyone is reinventing the wheel
  - Test setups show poor / no security
  - *"Vendors know what's good for us"*
    - We're talking about a critical application called border control...
- Entrust, which handles PKI security for ePassports, says that we should just trust them
  - *"Governments' security experts aren't dummies and they aren't going to make those mistakes"*



# Awareness, ct.

- So this doesn't seem to be a problem...
  - *“We know what we're doing”*
  - *“Just trust us!”*
- Security or dancing pigs?
  - Guess...

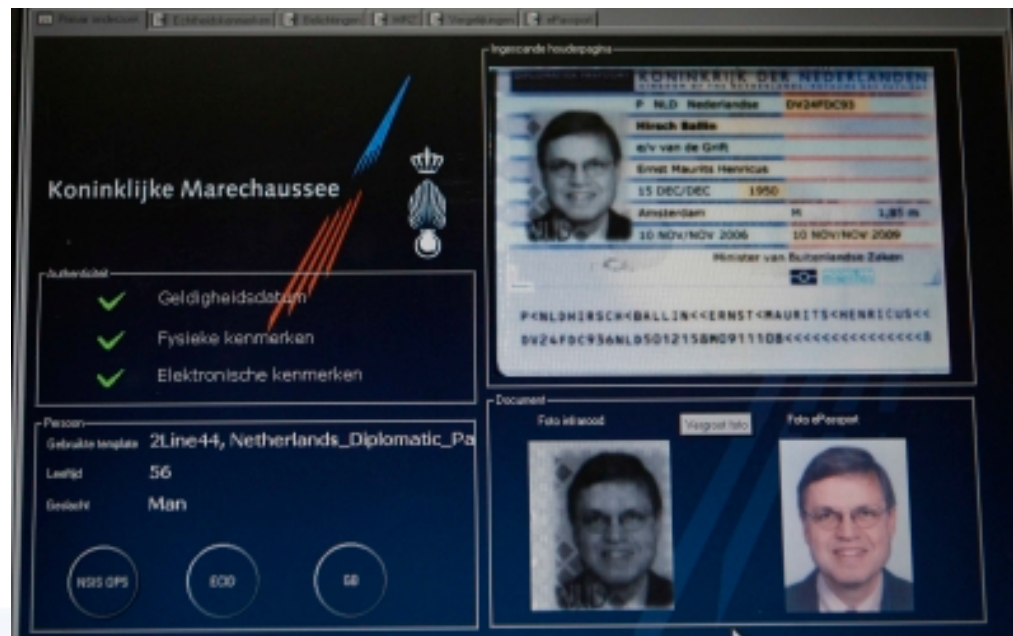






# Awareness, ct.

- Minister of justice Ernst Hirsch Ballin
  - Get it ultra high-res at [anp-photo.com](http://anp-photo.com)...



## Honderden paspoorten en identiteitskaarten gestolen bij Sdu

Van onze verslaggever Ferry Haan

gepubliceerd op 30 juni 2006 16:31, bijgewerkt op 1 juli 2006 08:16

Printversie

Deel dit artikel

AMSTERDAM - Er zijn honderden blanco paspoorten en identiteitskaarten gestolen bij de drukkerij Sdu Identification. De diefstal dateert van 2002, maar nadat de identiteitspapieren opdoken in het criminele circuit, is pas later aangifte gedaan. Dit bevestigt een woordvoerder van het ministerie van Binnenlandse Zaken.

Sdu Identification is het enige bedrijf in Nederland dat paspoorten mag maken. Het proces zou streng beveiligd moeten zijn. Het bedrijf mist echter 25 vellen met daarop elk 36 blanco identiteitskaarten. Ook zijn 155 stroken weg met telkens twee blanco houderpagina's voor in een paspoort.

De voormalige staatsdrukkerij Sdu verwijst door naar het ministerie voor een reactie op de diefstal. Volgens het ministerie werden in 2002 'telverschillen' ontdekt bij Sdu. Na onderzoek bleek dat medewerkers van Sdu hier niets mee te maken zouden hebben. De politie werd wel geïnformeerd, maar Sdu deed geen aangifte.

Dat gebeurde wel toen in 2004 de vervalste identiteitspapieren opdoken in het criminele circuit. Oplichters probeerden geld te incasseren, gebruik makend van de valse papieren.

Het ministerie betreurt dat paspoorten in handen zijn gevallen van criminelen. Volgens het

In 2002, 1.200 blank Dutch IDs were stolen. The printing company SDU did not officially report the crime(!) until the first documents were seen in the field in 2004...

'Nigeriaanse fraude'. De valse paspoorten zouden speciaal voor deze fraude gebruikt worden.

Het tv-programma RTL Nieuws zal vanavond aandacht besteden aan de paspoortendiefstal.

# EAC: the next generation

- Extended Access Control (EAC) is coming
  - In all EU ePassports starting 28 June 2009 (finger prints)
    - No international standard yet
    - Most countries seem to follow [BSI standard TR-03110 v1.11](#)
  - Chip Authentication
    - Active Authentication alike technology
  - Terminal Authentication
    - Terminal needs to be authorized to read sensitive data
      - Private key in terminal
      - Foreign terminal might also be authorized
        - » Exchanging *public* keys is still a problem (ICAO PKD)
        - » Now more complex schema and *private* keys
        - » Not authorized to read: no finger print check at all...
    - Terminal can update chip content
      - Denial of service [described](#) by Lukas Grunwald
  - Backward compatible
    - In many countries passports are valid for 10 years
      - EAC not fully effective until 28 June 2019...
      - Will criminals attack simple or advanced chips? Guess...



# Solutions

- Design (ICAO standard):
  - Require all security features including PKD by default
  - Document requirements for inspection systems
  - Protect the integrity of *all* files
- Implementation:
  - Use automated border control for chips with *all* security features enabled only
- Global coordination (e.g. ICAO or other UN body):
  - Provide standard implementation for ePassport applets and inspection systems
    - The more (black box) implementations, the higher the risk of a serious problem
    - Open standards and implementations, no security by obscurity!
  - Provide countries with a list of authorized hardware and hardware lifetimes
    - Think about the Mifare Classic chip family
    - History might repeat itself with ePassports: many travel documents are valid for 10 years. In 10 years the hardware is most probably outdated (DPA attacks etc.)
  - Enforce the use of a trusted PKI environment (PKD)
    - Automated real-time certificate & CRL checks



# Do it yourself

- Get my ePassport emulator @ <http://dexlab.nl/>
- Get software
  - eCLOWN (Nokia NFC) @ <http://dexlab.nl/>
  - RFIDIOT-vonjeek (PC) @ <http://freeworld.thc.org/thc-epassport/>
    - Fork of an old RFIDIOT version, most functionality is integrated in the latest RFIDIOT release
  - RFIDIOT (PC) @ <http://rfidiot.org/>
- Get hardware



RFID reader, ~ \$75



PC, ~ \$750



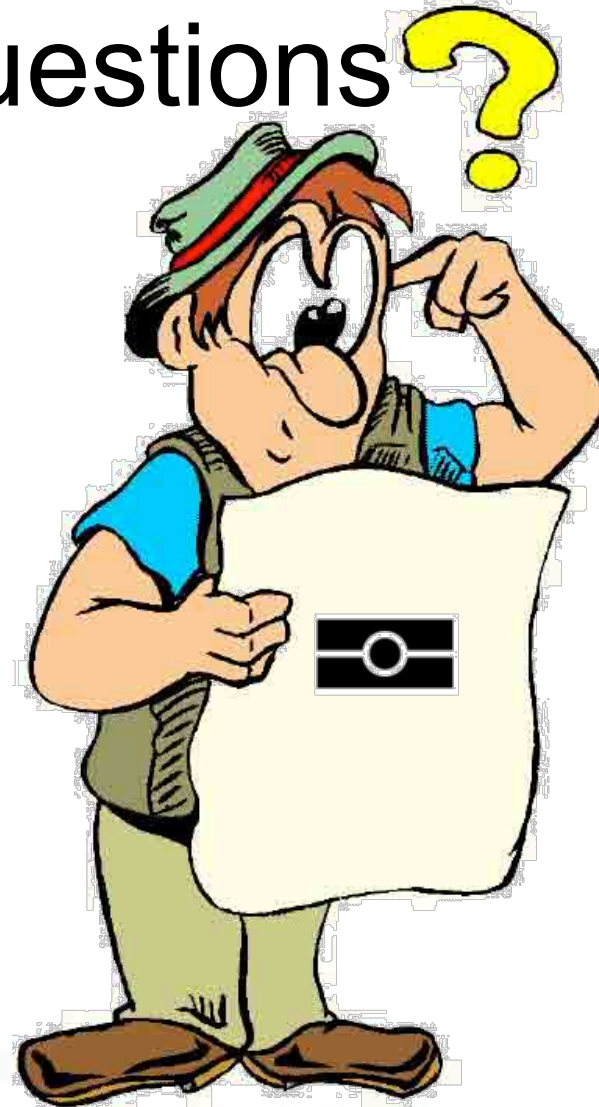
JCOP v4.1 72k, ~\$20



NFC phone, ~\$200



# Questions?



# Thank you!



## Contact details:



**dexlab**

it security audit, advisory & research

**J.C. (Jeroen) van Beek M.Sc CISSP CISA RE**

email: [jeroen@dexlab.nl](mailto:jeroen@dexlab.nl)  
internet: [www.dexlab.nl](http://www.dexlab.nl)



## Black Hat Briefings



# Further reading

- <http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>
- <http://www.timesonline.co.uk/tol/news/uk/crime/article4467098.ece>
- <http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witte-man.pdf>
- <http://www.wired.com/science/discoveries/news/2006/08/71521>
- <http://www.dice.ucl.ac.be/crypto/passport/index.html>
- <http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf>
- [http://www.theregister.co.uk/2008/09/30/epassport\\_hack\\_description/](http://www.theregister.co.uk/2008/09/30/epassport_hack_description/)
- <http://freeworld.thc.org/thc-epassport/>
- <http://www.dc414.org/download/confs/defcon15/Speakers/Grunwald/Presentation/dc-15-grunwald.pdf>
- <http://www.cs.auckland.ac.nz/~pgut001/pubs/biometrics.pdf>
- [http://www.cscs-si.gov.si/TR-PKI\\_mrtds\\_ICC\\_read-only\\_access\\_v1\\_1.pdf](http://www.cscs-si.gov.si/TR-PKI_mrtds_ICC_read-only_access_v1_1.pdf)
- <http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx>
- [http://www.bsi.de/literat/tr/tr03110/TR-03110\\_v111.pdf](http://www.bsi.de/literat/tr/tr03110/TR-03110_v111.pdf)
- [http://news.bbc.co.uk/2/hi/uk\\_news/7530180.stm](http://news.bbc.co.uk/2/hi/uk_news/7530180.stm)
- <http://www.telegraph.co.uk/news/newsttopics/howaboutthat/2456084/Grandmother-flies-to-Canary-Islands-on-her-husbands-passport.html>

