The Biometric Passport

The Swiss Case

Serge Vaudenay

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

http://lasecwww.epfl.ch/

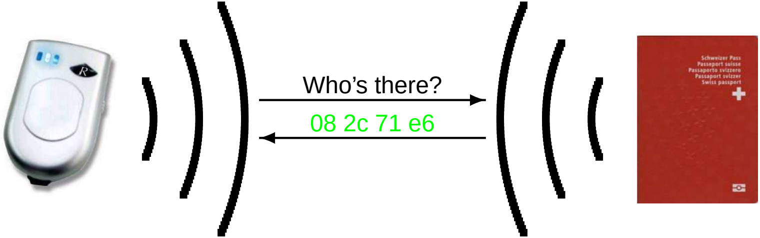
History & Political Background

- 1997 UN/ICAO (**International Civil Aviation Organization**) started to work on **machine-readable travel documents** (MRTD) based on **biometrics**
- 2004: ICAO MRTD standard release (now adopted by over 50 countries)
- 2006: EU extension (EAC)

- visa waiver for USA requires ICAO compliant passport
- Schengen agreement requires all passports to be biometric

▸ skip crypto

ISO 14443 (RFID)



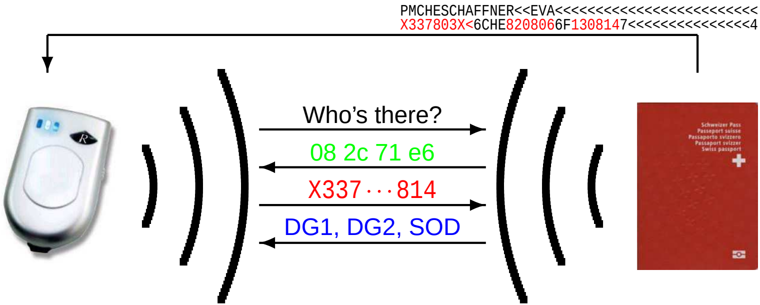
Who’s there?

08 2c 71 e6

- unauthorized radio access
- leaks ICAO implementation (passport presence)
- leaks chip’s model version (nationality)

ICAO (MRTD): BAC and Passive Authentication

```
PMCHESCHAFFNER<<EVA<<<<<<<<<<<<<<<<<<<<<<<<<
X337803X<6CHE8208066F1308147<<<<<<<<<<<<<<<4
```



Who's there?

08 2c 71 e6

X337 · · · 814

DG1, DG2, SOD

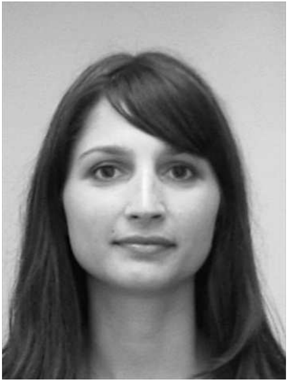
- unlimited access based on printed access key
- leaks biometric template for automatic identification
- leaks evidence of correct identity (digital signature)

An Identity Example

DG1

```
PMCHESCHAFFNER<<EVA<<<<<<<<<<<<<<<<<<<<<<<<<<
X337803X<6CHE8208066F1308147<<<<<<<<<<<<<<<4
```

DG2



SOD

Digests:

DG1: `4e1249fb72c8e70ba72f488dc1f91394e57f9f83`

DG2: `a3853c3c8261c2788fc2c4b9db372c5875f5c91d`

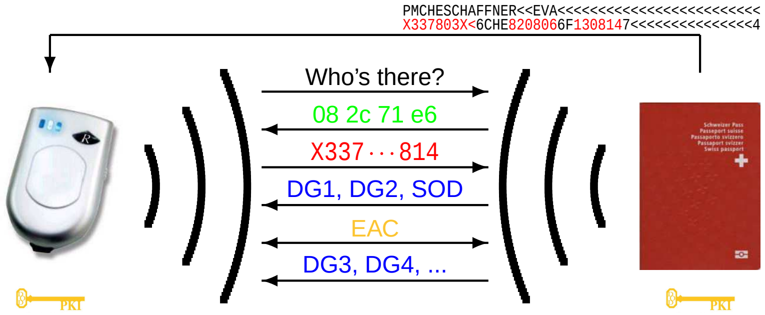
Signature:

```
54a4 a626 4ee1 c0ab e022 3f1d e673 75d4
7c89 7e7f d8fb acd6 abbf d568 b178 7171
652d e730 43c2 9495 6134 680c 7070 9028
1caa 2364 17e8 ffa0 9ee7 c8be 4c32 908c
```

Certificate:

```
MIIECTCCA5GgAwIBAgIBFDAJBgcqhkjOPQQBMHExCzAJBgNVBAYTAkNIMQ4wDAYD
VQQKEwVBZG1pbjERMA8GA1UECxMIU2VydmljZXMxIjAgBgNVBAsTGUNlcnRpZmlj
YXRpb24gQXV0aG9yaXRpZXMxGzAZBgNVBAMTEmNzY2Etc3dpdHplcmxhbmQtMTAe
Fw0wODA1MTkwODA4NDVaFw0xNDA2MjEwODA4NDVaMG0xCzAJBgNVBAYTAkNIMQ4w
DAYDVQQKEwVBZG1pbjERMA8GA1UECxMIU2VydmljZXMxGTAXBgNVBAsTEFNpZ25h
dHVyZS1TZXJ2ZXIxDzANBgNVBAsTBlBhc3MwNjEPMA0GA1UEAxMGZHMtMDAxMIIB
MzCB7AYHKoZIzj0CATCB4AIBATAsBgcqhkjOPQEBAiEA/////wAAAAEAAAAAAAAA
AAAAAAD///////////////8wRAQg/////wAAAAEAAAAAAAAAAAAAAAD/////////
//////wEIFrGNdiqOpPns+u9VXaYhrxlHQawzFOw9jvOPD4n0mBLBEEEaxfR8uEs
Qkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpZP40Li/hp/m47n60p8D54WK84zV2sx
Xs7LtkBoN79R9QIhAP////8AAAAA//////////+85vqtpxeehPO5ysL8YyVRAgEB
A0IABO8J8UthgahfN1JQKIq9a1ll/L3er54mUd1SZMnKQ2pQTbX5JwHc9ByEgw3G
5kucfGw1k2uAts+Ck+WSovy7k7GjggFBMIIBPTArBgNVHRAEJDAigA8yMDA4MDUx
OTA4MDg0NVqBDzIwMDgwODIwMDgwODQ1WjBgBgNVHSAEWTBXMFUGCGCFdAERAzQB
MEkwRwYIKwYBBQUHAgEWO2h0dHA6Ly93d3cucGtpLmFkbWluLmNoL3BvbGljeS9D
UFNfMl8xNl83NTZfMV8xN18zXzUyXzEucGRmMIGbBgNVHSMEgZMwgZCAFE7InZjJ
tOCQ9StbhZdQVr/oJOt2oXWkczBxMQswCQYDVQQGEwJDSDEOMAwGA1UEChMFQWRt
aW4xETAPBgNVBAsTCFNlcnZpY2VzMSIwIAYDVQQLExlDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0aWVzMRswGQYDVQQDExJjc2NhLXN3aXR6ZXJsYW5kLTGCAQEwDgYDVR0P
AQH/BAQDAgeAMAkGByqGSM49BAEDZwAwZAIwGYMbTqjlYQnJ1DSpb//5WtQthjoy
pGrbBZW1Rqa7TXffzQX818OjQCdQ0n9tZEDlAjBPtMdS9OymxywZpXZj9Os2qO6M
6htXJKXpdKSWq75ZhQRet/or3pT2MQ56n69hqGw=
```

EU (EAC): Access Control and Active Authentication



```
PMCHESCHAFFNER<<EVA<<<<<<<<<<<<<<<<<<<<<<<<<<
X337803X<6CHE8208066F1308147<<<<<<<<<<<<<<<<4
```

Who’s there?

08 2c 71 e6

X337 · · · 814

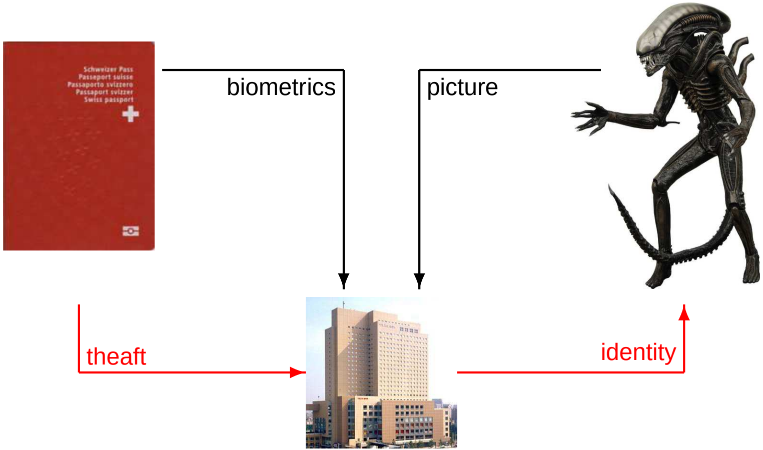
DG1, DG2, SOD

EAC

DG3, DG4, ...

- access granted based on bilateral agreements
- protects only the fingerprint
- comes after mandatory ICAO leakages

Identity Theaft



biometrics

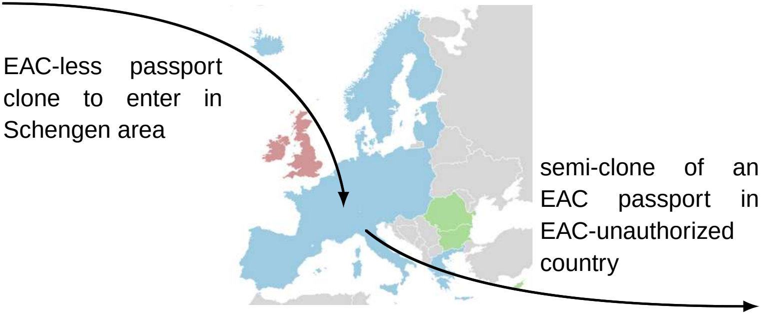
picture

theaft

identity

a few hundreds of customers suffice

Limited Anti-Cloning Protection



EAC-less passport clone to enter in Schengen area

semi-clone of an EAC passport in EAC-unauthorized country

The Swiss Case

Swiss Government, 2008 June 13

- all identity documents may have a chip with e-identity
- may be used for authentication, signature, and encryption
- government specifies the required security level
- government can authorize access by other countries
- government may authorize access by transport companies
- central database with all data from the chip
- available to the police, border control, government authorities

The Swiss Bug

- if we can find 50 000 people upset about a new law within a given delay, the law goes to popular referendum
- referendum schedules on 2009 May 17
- first time people will have to vote on this issue!

Political Campaign

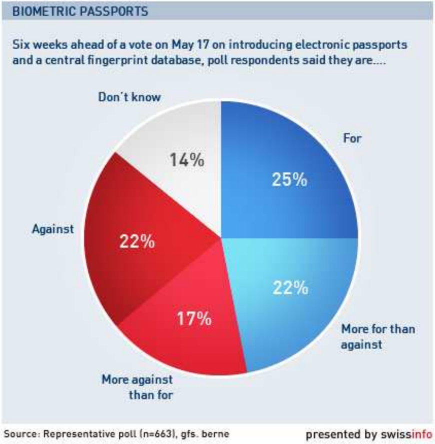
Yes to Traveling Freedom

No to Mandatory Biometrics

No to Citizen Filings

Yes to Individual Freedom

Poll (Early April 2009)



BIOMETRIC PASSPORTS

Six weeks ahead of a vote on May 17 on introducing electronic passports and a central fingerprint database, poll respondents said they are....

Source: Representative poll (n=663), gfs. berne

presented by swissinfo

Conclusion

- watch on Swiss news on May 17