

Security Challenges in RFID Passports

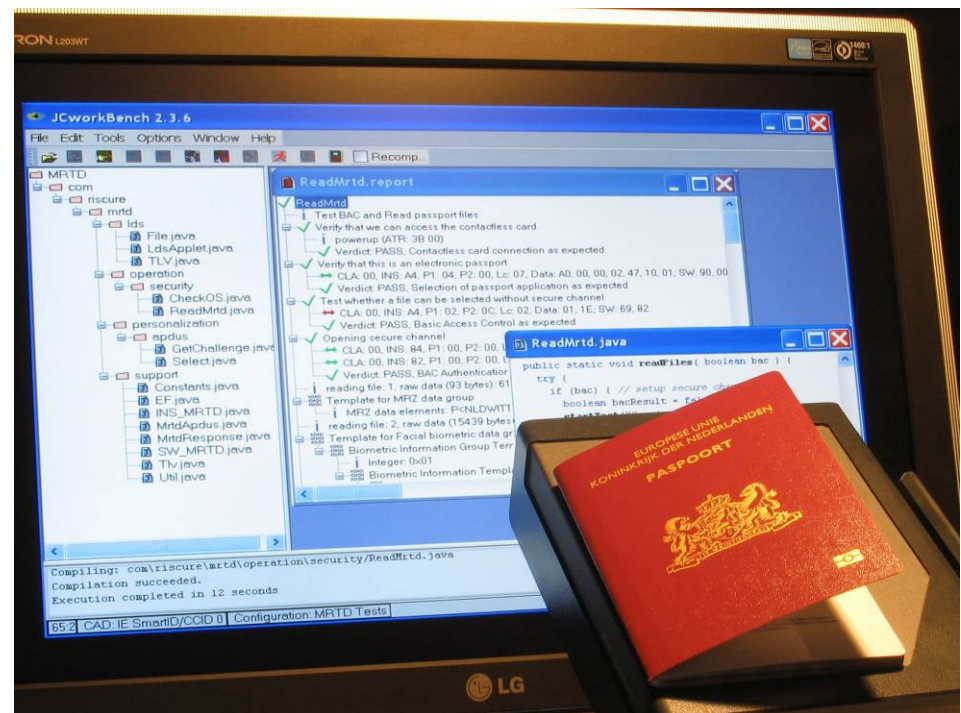
GovCert conference
October 18, 2007

Harko Robroch
Managing Director

Our involvement in electronic passports



- Published weakness in BAC static key in July 2005
- Performed security testing on electronic passport technology



- Read the public standards from ICAO
- Read other public sources
 - International Civil Aviation Organisation web site on MRTDs: <http://mrtid.icao.int/>
 - Riscure, publication of BAC weakness, July 2005:
http://www.riscure.com/2_news/passport.html
 - FIDIS Budapest Declaration, Sep 2006:
<http://www.fidis.net/press-events/press-releases/budapest-declaration/>
 - BSI Technical Guideline - Extended Access Control, Feb 2006:
http://www.bsi.bund.de/fachthem/epass/EACTR03110_v101.pdf
 - Security Document World on Extended Access Control:
http://www.securitydocumentworld.com/client_files/eac_white_paper_210706.pdf
 - Crossing Borders paper, J.H. Hoepman et al, Oct 2006:
<http://www.cs.ru.nl/~bart/PAPERS/index.html>
- Play around with chip technology ...

Test your own passport at Schiphol

- Public access to a reader
- Displays personal info from chip



And, our pig showed on-screen 😊



Public reader at Schiphol does not verify the certificate, but only displays the info



- **How the security works**
- Can the chip be cloned?
- Security challenges
- Conclusion

What are the issues?



1. **Passport forgery**

- Criminal organization makes a false passport
- High-tech and more difficult

2. **Look-alike fraud**

- Criminal organization steals many passports
- Look for the best match
- Low-tech and relatively easy

1. To address passport forgery

- A certificate with passport holder data (passive auth)
- A private key on a smart card (active auth)

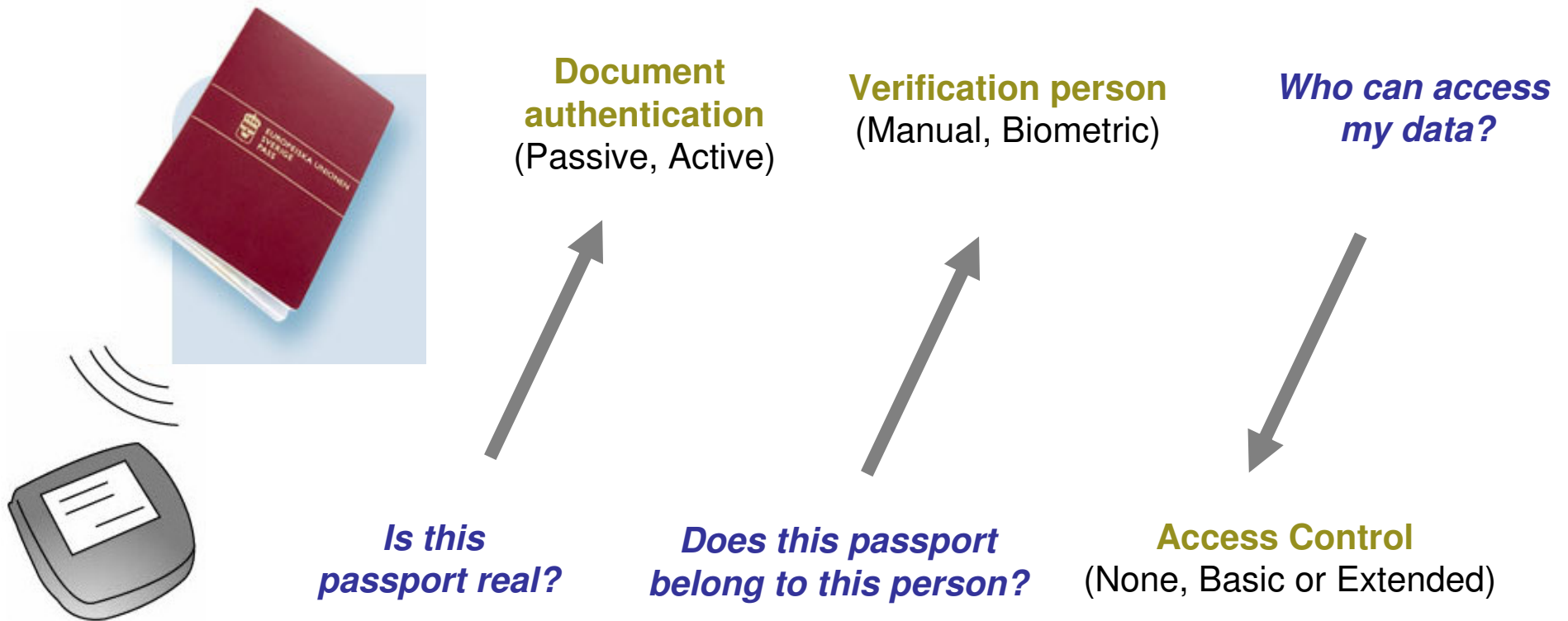
2. To address look-alike fraud

- Personal biometric data on the chip
- To reduce *false accepts*
- Does it work?

And introduces contactless chip technology ...



Protection mechanisms in ICAO

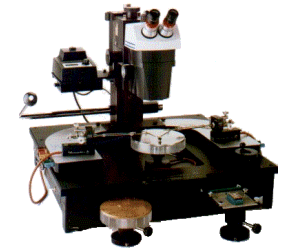
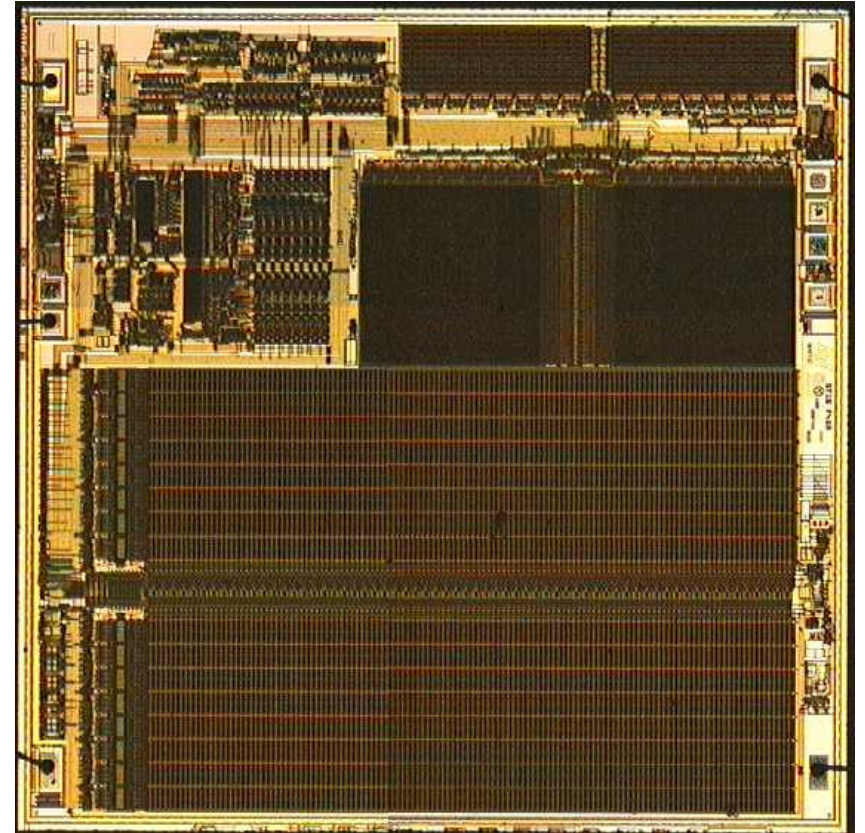
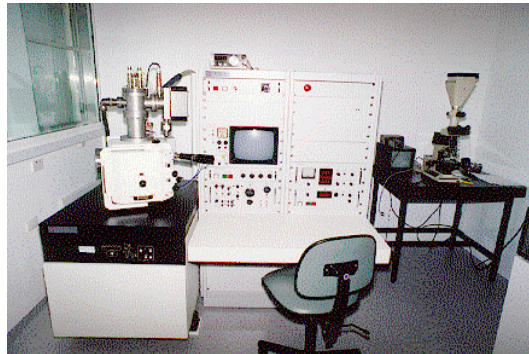
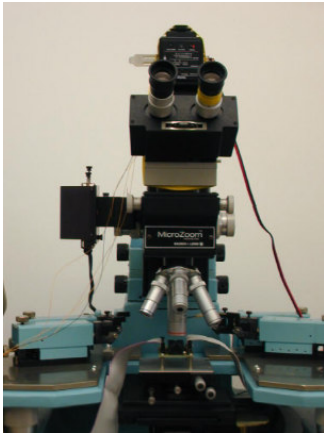
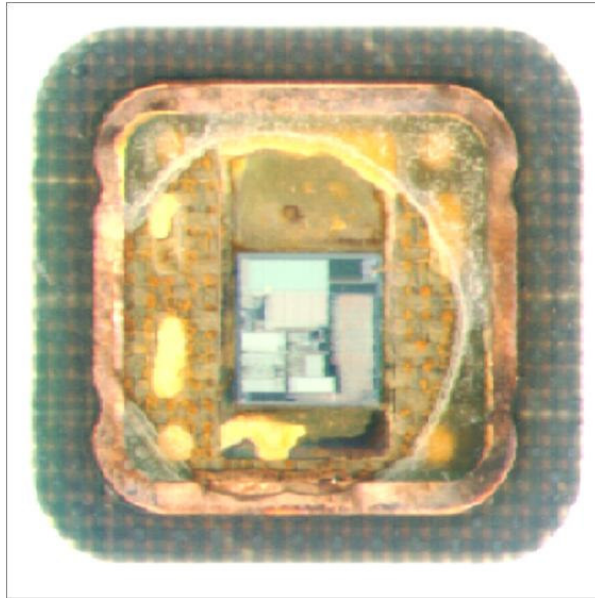


- How the security works
- **Can the chip be cloned?**
- Security challenges
- Conclusion

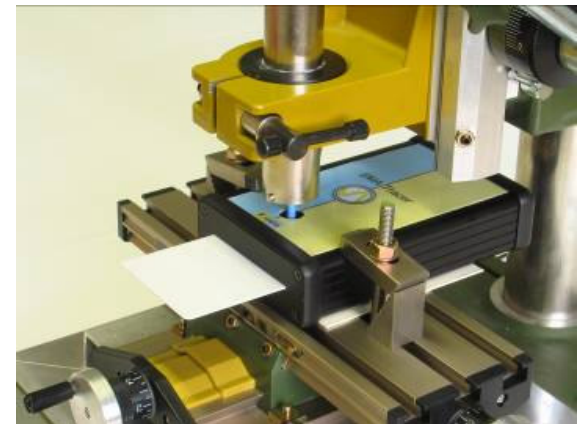
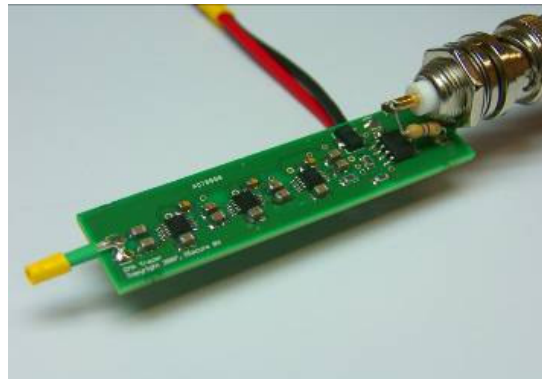
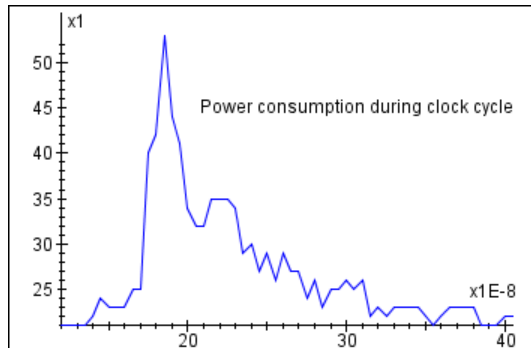
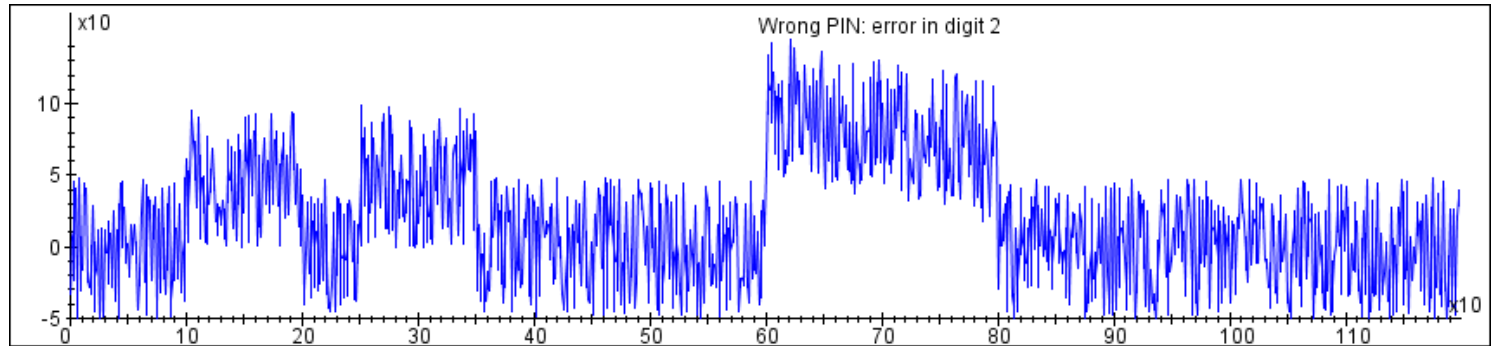
- Cloning usually implies copying the secret
 - Secret key in Active Authentication
 - **No secret** in Passive Authentication !
- Fortunately, Dutch passport **uses Active Authentication**

- So, how would one try to get the secret?
 1. **Invasive** methods, open the lid
 2. Attack by abusing a **side channel**
 3. Abuse the application protocol

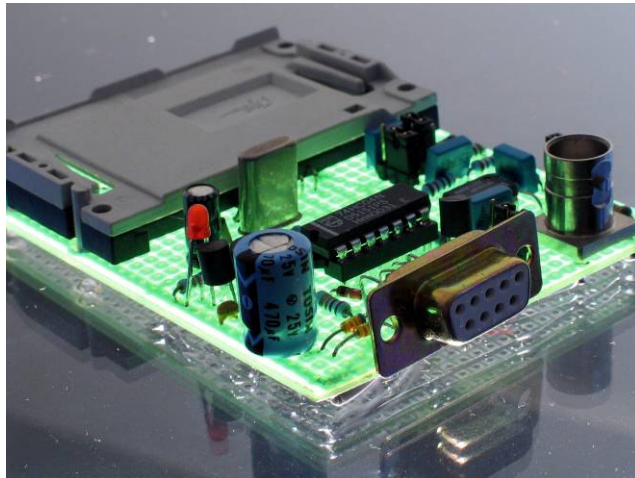
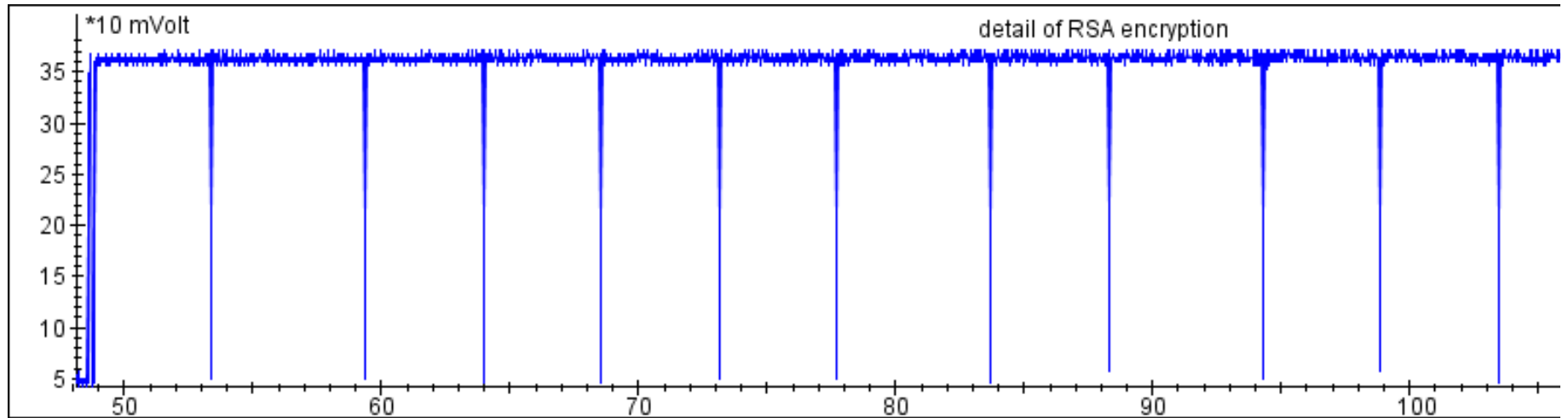
Skills, equipment and time



Skills, equipment and time



Skills, equipment and time



Often cheap equipment also works!

But, many countermeasures in chip



- **Hardware**

- shielding
- active light & heat sensors
- reduce signal strength
- add amplitude and timing noise

- **Operating system**

- random delays and random ordering of independent processes
- algorithmic variations
- verification traps

- **Application**

- retry counters
- session keys
- limited control and visibility of crypto input and output
- leakage proof program flow

Smart cards can offer a very high level of protection

- How the security works
- Can the chip be cloned?
- **Security challenges**
 - BAC
 - Trusting a country certificate
 - Certificate validation
 - Contactless chip
- Conclusion


Weakness in Basic Access Control



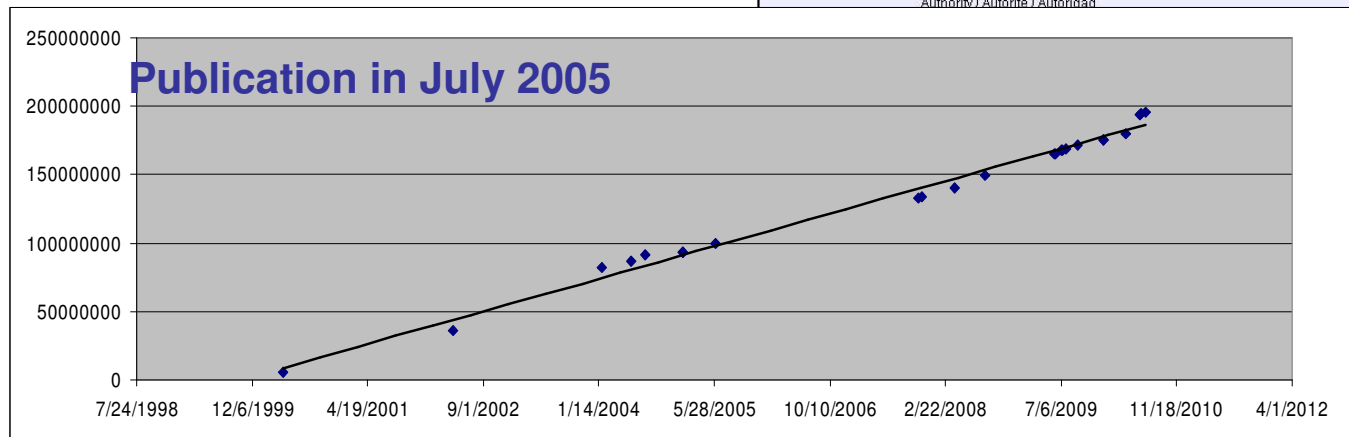
Static access key is derived from MRZ data

- **Date of birth**
- **Date of expiry**
- **Passport number**

PASSPORT PASSEPORT PASAPORTE	Type / Type / Tipo P Code / Code / Código UTO Passport No. / No. du Passeport / No. de Pasaporte L898902C Surname / Nom / Apellidos ERIKSSON Given names / Prénoms / Nombres ANNA MARIA Nationality / Nationalité / Nacionalidad UTOPIAN Date of birth / Date de naissance / Fecha de nacimiento 06 Aug 1969 Personal no / no personnel Z5192169 Sex / Sexe / Sexo F Place of birth / Lieu de naissance / Lugar de nacimiento ZENITH, UTOPIA Date of Issue / Date de délivrance / Fecha de expedición 24 Jun 1989 Authority / Autorité / Autoridad	UTOPIA
---	---	---------------



Predictability & dependency reduce Entropy to 35 bits



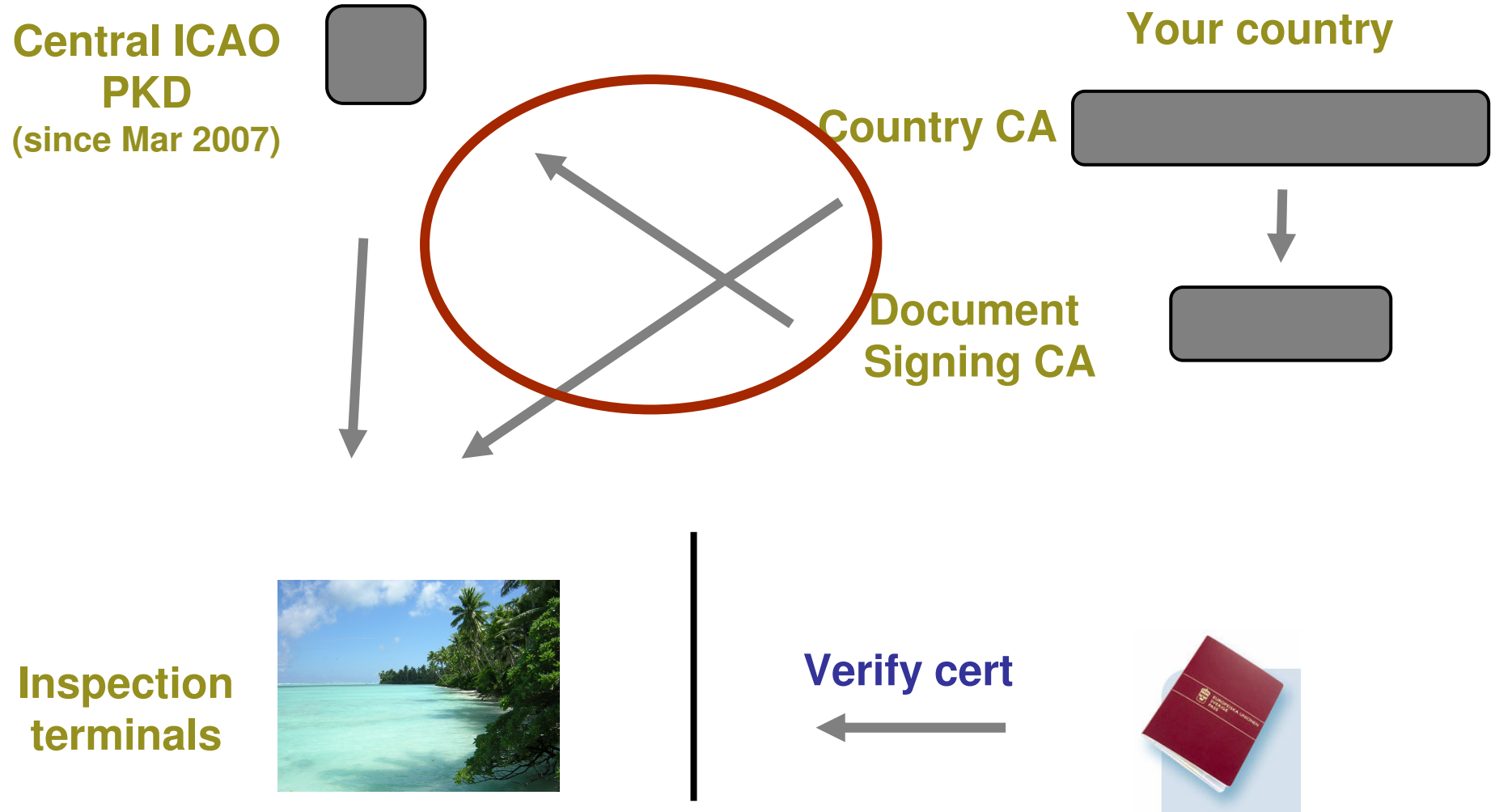
Is 35 bit sufficient to protect personal data?

Solution

- Country can use unpredictable passport numbers
- **But**, protection remains limited due to **static key** that is **visible for any person** who had access to the passport

At launch in Aug 2006, Dutch passport moved to unpredictable numbers to reach entropy of 66 bits

Trusting a country certificate (PA)

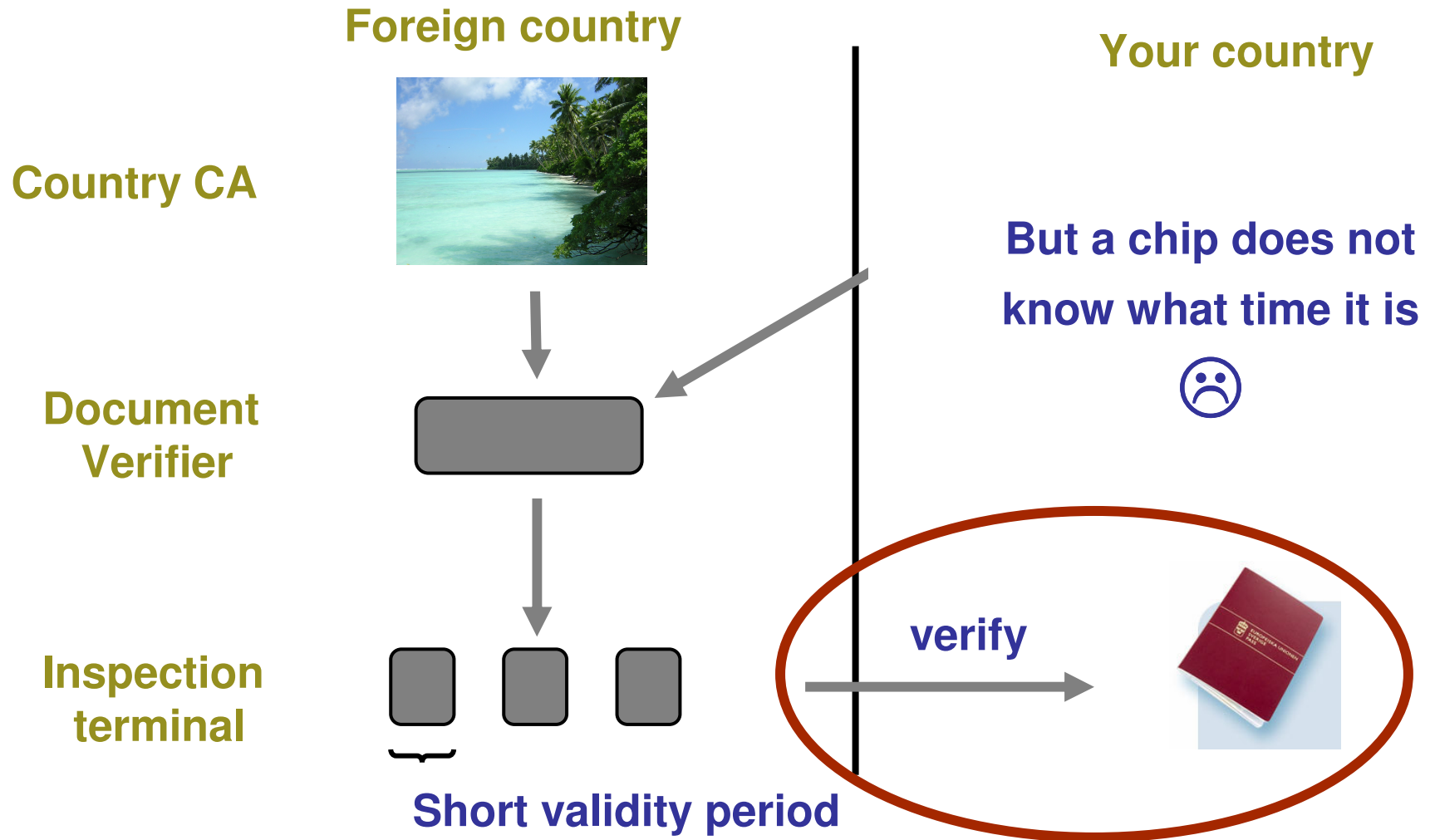


Extended Access Control (EAC)

- To access **most sensitive** data on chip (e.g. biometric data in future)
- Implements mutual authentication



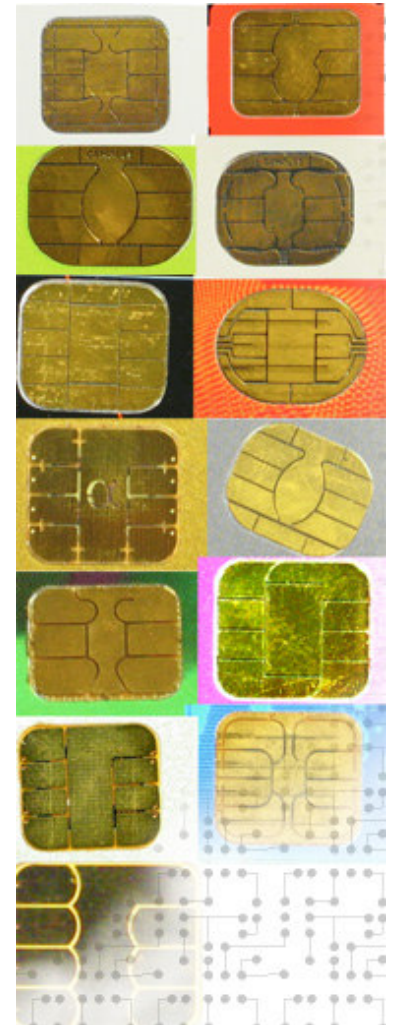
Certificate infrastructure EAC



Use of *contactless* technology appropriate?

- Introduces access and eavesdropping issues
- Sometimes, shielding is applied (e.g. USA)
- Contact-based chip technology eliminates several issues

→ Dutch eNik will use contact-based smart card



- How the security works
- Can the chip be cloned?
- Security challenges
- **Conclusion**

The electronic passport ...



1. Provides **good forgery** protection
2. Introduces **privacy concerns with RF**

We did not talk about look-alike fraud

... how **effective** are fingerprint biometrics in addressing this?

... how much of a **challenge to privacy** requirements?

Thank you. Questions?

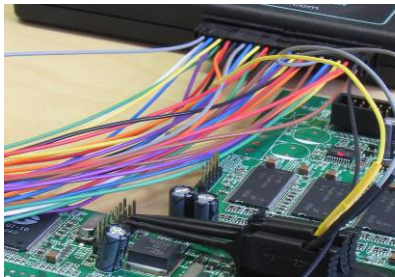


Harko Robroch
Managing Director
robroch@riscure.com



Riscure B.V.
Rotterdamseweg 183c
2629 HD Delft
The Netherlands

Phone: +31 (0)15 2682664
[Http://www.riscure.com](http://www.riscure.com)



**CHALLENGE
YOUR SECURITY**

