Security by Politics - Why it will never work

Lukas Grunwald

DN-Systems GmbH Germany

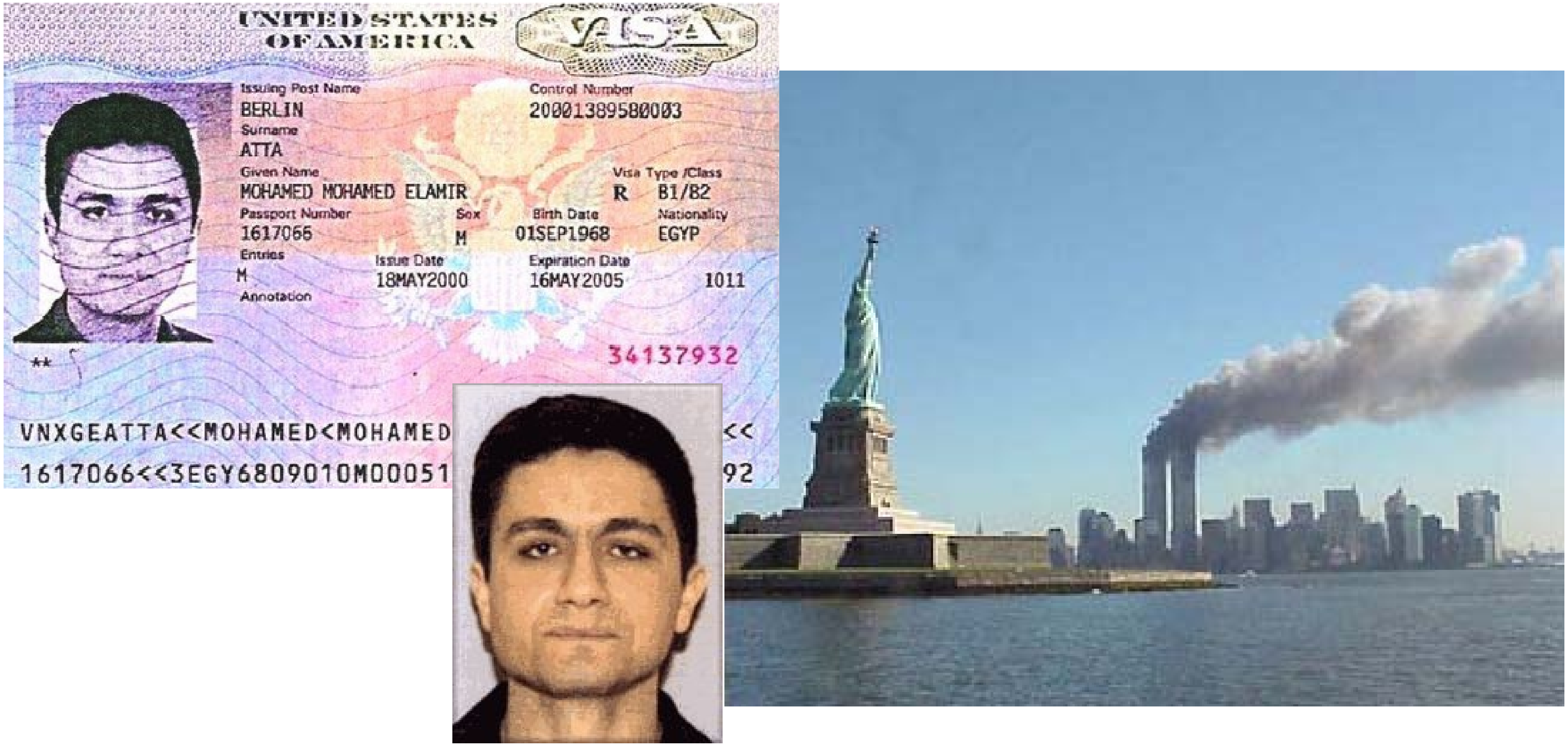
DefCon 15 – Las Vegas

USA

Agenda

- Motivation
- Some basics
- Brief overview ePassport (MRTD)
- Why cloning?
- How to attack the system
- BAC (Basic Access Control)
- EAC (Extended Access Control)
- Enrollment: Unexpected risks

Motivation - MRTD



UNITED STATES OF AMERICA

VISA

Issuing Post Name BERLIN		Control Number 20001389580003	
Surname ATTA			
Given Name MOHAMED MOHAMED ELAMIR		Visa Type /Class R B1/B2	
Passport Number 1617066	Sex M	Birth Date 01SEP1968	Nationality EGYP
Entries M	Issue Date 18MAY2000	Expiration Date 16MAY2005	1011
Annotation			

**

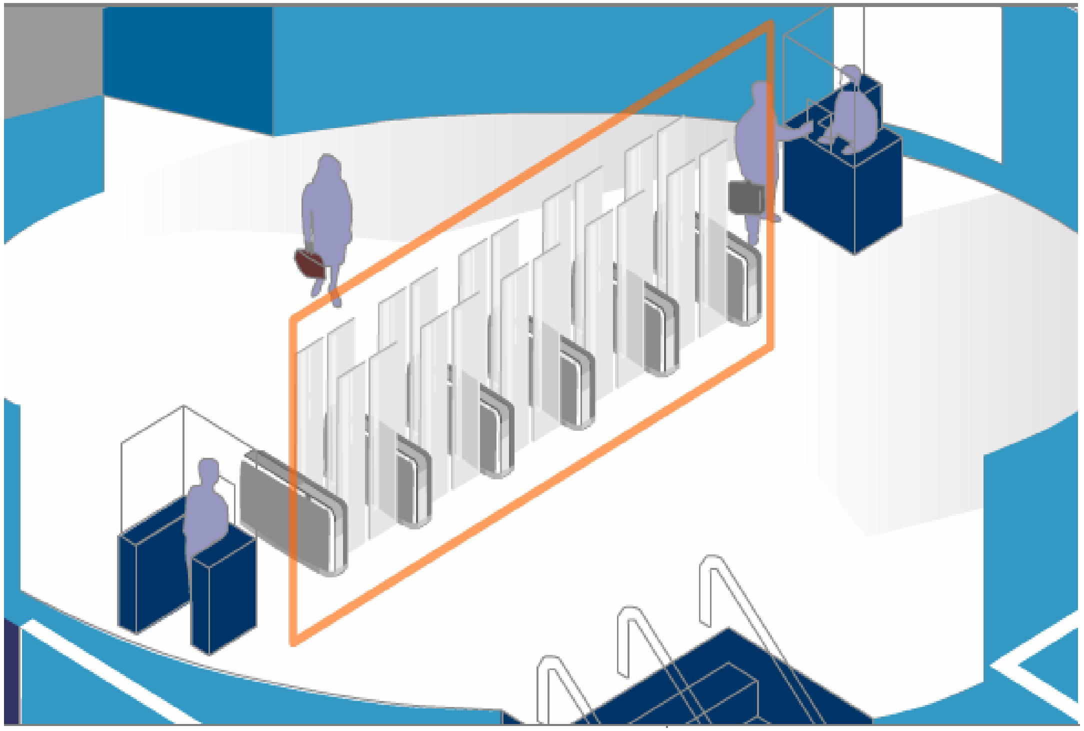
34137932

VNXGEATTA<<MOHAMED<MOHAMED <<

1617066<<3EGY6809010M00051 92

This image is a work of a Federal Bureau of Investigation employee, taken or made during the course of an employee's official duties. As a work of the U.S. federal government, the image is in the ***public domain****.*

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 ePassport

- 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
  - JEPG or JEPG2000
- Same with fingerprints
- Compromises don't work with security

ePassports

This image is a work of a United States Department of Homeland Security employee,
taken or made during the course of an employee's official duties.
As a work of the U.S. federal government, the image is in the public domain.

MRTD

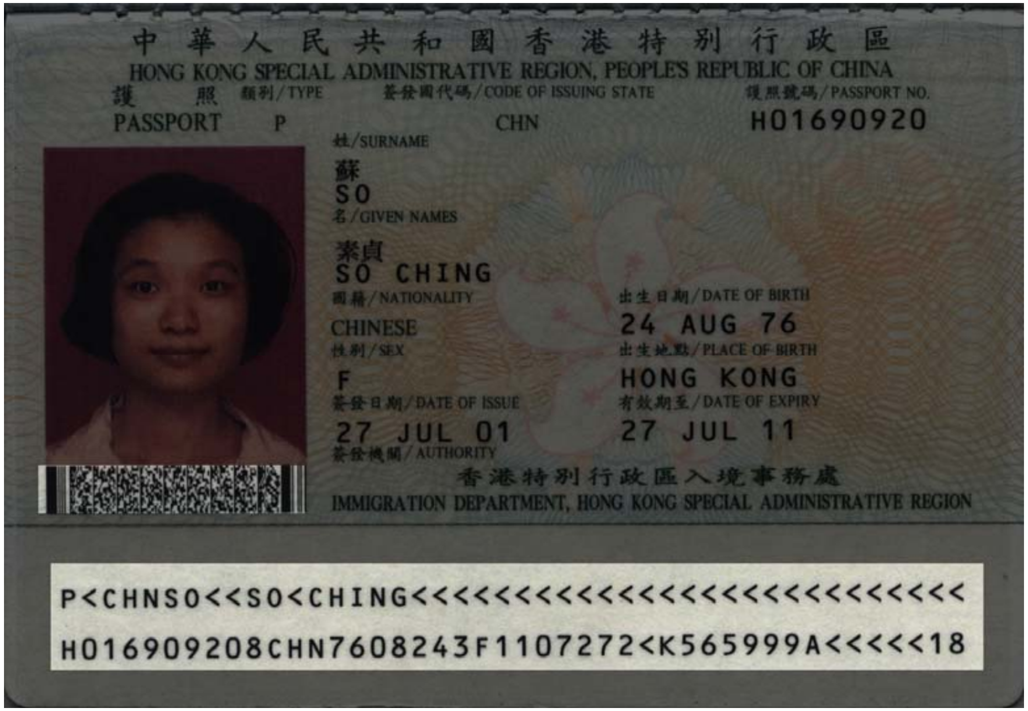
- Machine Readable Travel Document aka Electronic Passports (ePassports)
- Specifications by ICAO
  - (International Civil Aviation Organization)
- Enrollment on a global basis

ePass from Germany

Quelle: Bundesministerium des Innern

- RFID tag embedded into the cover
- Produced by the Bundesdruckerei GmbH
- No shield, readable even when passport cover is closed

2D Code and MRZ



中華人民共和國香港特別行政區
HONG KONG SPECIAL ADMINISTRATIVE REGION, PEOPLE'S REPUBLIC OF CHINA

護照 PASSPORT

類別/TYPE: P

簽發國代碼/CODE OF ISSUING STATE: CHN

護照號碼/PASSPORT NO.: H01690920

姓/SURNAME: 蘇 SO

名/GIVEN NAMES: 素貞 SO CHING

國籍/NATIONALITY: CHINESE

出生日期/DATE OF BIRTH: 24 AUG 76

性別/SEX: F

出生地點/PLACE OF BIRTH: HONG KONG

簽發日期/DATE OF ISSUE: 27 JUL 01

有效期至/DATE OF EXPIRY: 27 JUL 11

簽發機關/AUTHORITY: 香港特別行政區入境事務處
IMMIGRATION DEPARTMENT, HONG KONG SPECIAL ADMINISTRATIVE REGION

```
P<CHNSO<<SO<CHING<<<<<<<<<<<<<<<<<<<<<<<<<<<
H016909208CHN7608243F1107272<K565999A<<<<<18
```

Passport with 2D barcode and MRZ (machine readable zone)

MRTD Data-Layout

- LDS (Logical Data Structure)
  - Data is stored in DG (Data Groups)
    - DG1: MRZ information (mandatory)
    - DG2: Portrait image + biometric template (mandatory)
    - DG3-9: Fingerprints, iris image (optional)
    - EF.SOD: Security Object Data (cryptographic signatures)
    - EF.COM: List of existing Data Groups
- Data is stored BER-encoded like ASN.1
- DG2-DG4 uses CBEFF for encoding

  (Common Biometric File Format, ISO 19785)

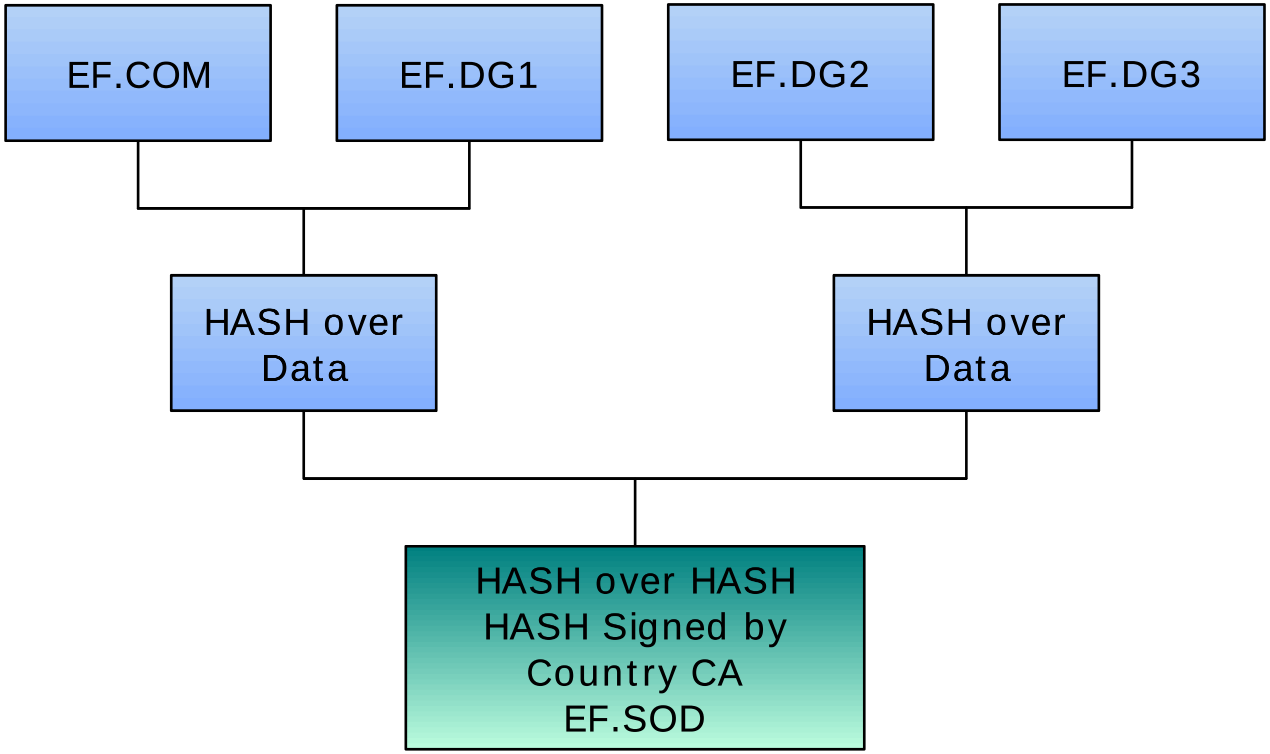
MRTD Security Features

- 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

Passive Authentication

- This method is mandatory for all passports
- Method of proof that the passport files are signed by issuing country
- Inspection system to verify the hash of DG's
  - EF.SOD contains individual signatures for each DG
  - EF.SOD itself is signed
  - Document signer public key from PKD / bilateral channels
  - Document signer public key can be stored on the passport
  - Useful only if country’s root CA public key known

Signed Data



EF.COM

EF.DG1

EF.DG2

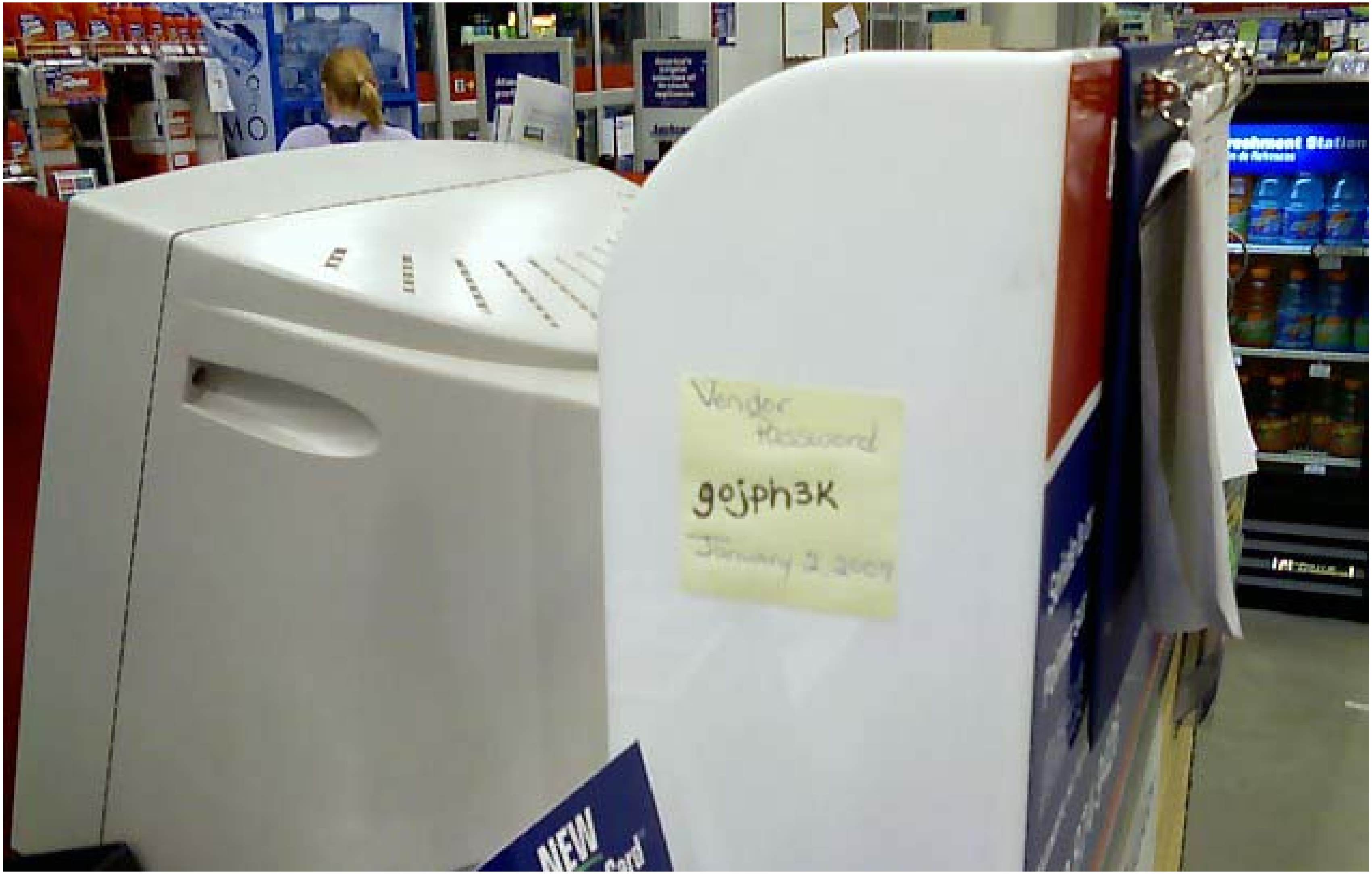
EF.DG3

HASH over Data

HASH over Data

HASH over HASH
HASH Signed by Country CA
EF.SOD

Password on Monitor?



Basic Access Control

- Grants access to data after inspection systems are authorized
- Authorization through the Machine Readable Zone (MRZ)
  - Nine digit document number
  - In many countries: issuing authority + incrementing number
  - Six digit date of birth
    - Can be guessed or assumed to be a valid date
  - Six digit expiry date
  - 16 most significant bytes of SHA1-hash over MRZ_info are used as 3DES key for S/M (ISO7816 secure messaging)
- Some European passports (Belgium) don’t have BAC

BAC

- The access key is printed on the passport
- Many times the passport is put on a Xerox machine in:
  - Hotels
  - Rentals (cars, ski, …)
  - Shops (cell phones, ...)
- The data from the MRZ is stored in many private databases (airlines, banks …)

BAC And Traceability

- With the BAC handshake data known,
  - the random unique ID is worthless
  - the MRTD is traceable
  - access to the content (LDS-DG.1 &DG.2) is possible
  - access to the SOD is possible

Extended Access Control

- Optional method (EAC)
- Should prevent the unauthorized access to biometric data
  - Not internationally standardized
  - Implemented only by individual issuers
  - Only shared with those countries that are allowed access
- Access is only possible with certificates from issuing country

Where is my clock?

Inspection of CV-Certs

- The MRTD does not have any reliable and secure time information
- Once a CV is captured, all MRTDs which have been read using a CV issued earlier could be accessed
- The biometric data is accessible as well
- The MRTD can not verify the validity of the timestamp from a CV certificate
- A false CV certificate with an issue date far out in the future can deactivate the MRTD permanently

EAC Risks

- A false CV certificate can deactivate the MRTD permanently
- A rogue regime could misuse the CV certificates to obtain fingerprints from passport holders
- With these fingerprints it is possible to produce false evidence

PKI Integration

- X.509 Certificates
  - Every issuer operates a self-controlled CA
  - Signer keys are derived from CA root
  - Public keys are distributed via ICAO PKD
  - Everyone can verify
  - **It is not possible to revoke a certificate on the MRTD**

Why Cloning of Passports?

- 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” ePassport
- Cloned tag could be extended with exploits
- Exploit could attack inspection system, backend or databases

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

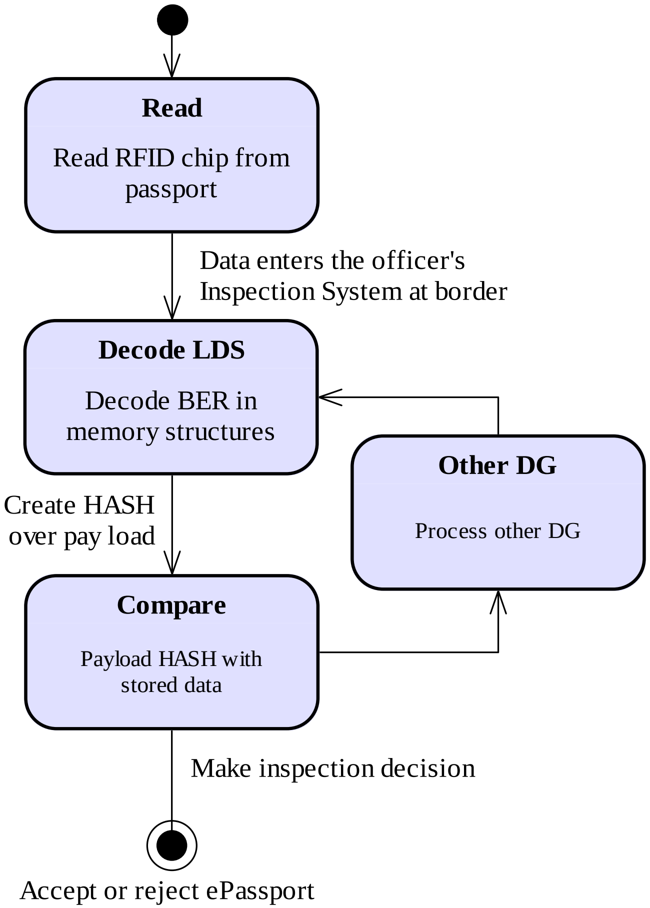
A Vendor’s Design of an Inspection System

dn Systems

- 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

Designed for Microsoft® Windows® XP

Problem With The Procedure



Read
Read RFID chip from passport
Data enters the officer's Inspection System at border
Decode LDS
Decode BER in memory structures
Other DG
Process other DG
Create HASH over pay load
Compare
Payload HASH with stored data
Make inspection decision
Accept or reject ePassport

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

Biometric Data

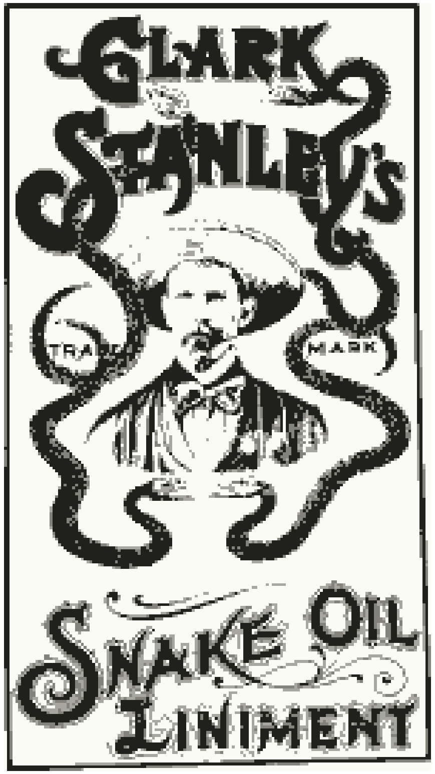
- Data should be reduced to hashes only
- But fingerprints will be stored as pictures
- Reverse-engineering of fingerprints possible with MRTD data
- Contrary to any best practice in IT security

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

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 version of this presentation 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

dn Systems

Questions?