e-passports

Erik Poll

Digital Security Group

Radboud University Nijmegen

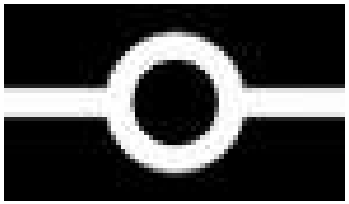
overview

- e-passports
- functionality and security mechanisms
- problems, so far
- future

e-passports

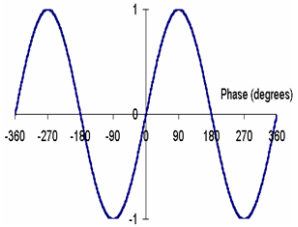
- e-passport contains RFID chip / contactless smartcard
  - in Dutch passports, a Java Card
- chip stores digitally signed information:
  - initially just facial images (photos)
  - also fingerprints
  - later maybe iris
- aka biometric passport or MRTD with ICC/chip

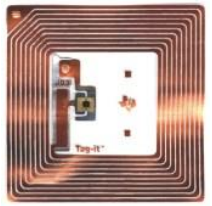
- introduction pushed by US in the wake of 9/11
  - to solve what problem??



e-passport logo

Protocols & standards





ISO 14443

- defines physical communication for RFIDs

ISO 7816

- originally developed for contact smartcards
- defines standard APDU commands & responses,

ICAO standard for e-passports

- defines specific IS0 7816 commands and responses for passports

additional EU standards

- standardise optional parts of ICAO specs
- additional advanced secuity mechanisms on top of ICAO

optical vs electronically readable

NB possible confusion

MRTD = Machine-Readable Travel Document
just has Machine (OCR) Readable Zone,
the MRZ, but need not contain a chip

so

e-passport = MRTD + chip

MRZ

e-passports & authentication

- authentication of data
- authentication of the chip
- authentication of the terminal
- authentication of the passport holder
  - how?
    - passport data: age, height, gender,...
    - facial image, fingerprint, iris
    - signature

Biometrics to authenticate passport holder

- Facial image (DG2, ISO 19794-5)
  - JPEG or JPEG2000 image
- Fingerprint (DG3, ISO 19794-1)
  - Uncompressed, WSQ, PNG, JPEG or JPEG2000
  - How to indicate the fingerprint cannot be enrolled (no DG3, empty DG3, no template), how to store 2 fingerprints (2 images, 2 templates)
- Iris image (DG4, ISO 19794-6)
- NB one would prefer not to store the raw biometrics, but some (hash of) derived info. *Why? How?*

Security mechanisms

- Passive Authentication (PA)
  - digital signature on passport data on chip
- Basic Authentication Control (BAC)
  - access control to chip, to prevent unauthorised access & eavesdropping
- Active Authentication (AA)
  - chip authentication
    - ie prevent cloning
- Extended Access Control (EAC)
  - chip and terminal authentication

ICAO mandatory

ICAO optional, EU mandatory

ICAO optional

EU only, mandatory for 'advanced' biometrics, ie fingerprint & iris

Passive Authentication

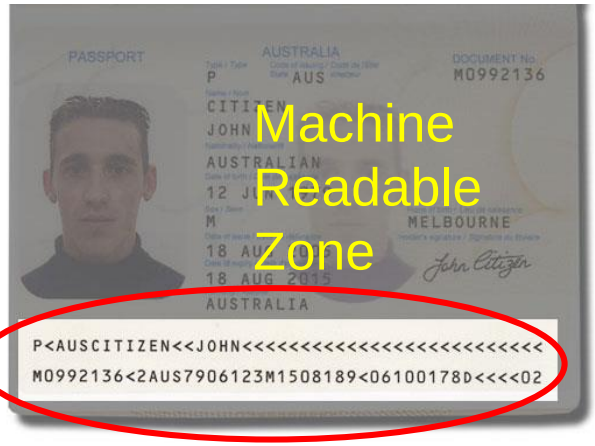
- passport chip consists of 16 data groups (DGs)
  - DG1 MRZ
  - DG2 face
  - DG3 finger
  - DG4 iris
  - ...
  - DG15 Active Authentication
  - ...

  and security object SO: signed hash values of the data groups
- To check the signatures, terminal needs country signing certificates
- Passive Authentication mandatory on all e-passports

Basic Access Control (BAC)

protects against unauthorised access and eavesdropping

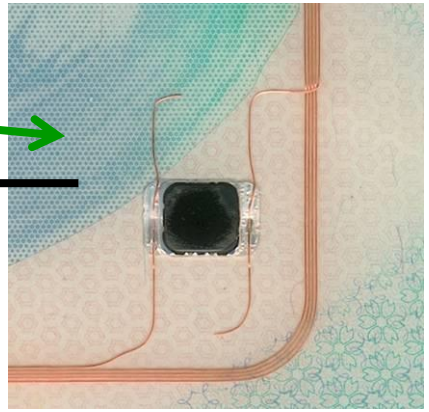
optically read MRZ



send MRZ

receive additional info

encrypted



Basic Access Control (BAC)

- BAC ensures data can only be read *after* reader proves knowledge of the MRZ of the passport
  - which “”proves” consent by the passport holder
  - funny but useful idea: *the password is written in the passport!*
  - The authentication key is derived from document nr, date of birth, date of expiry
- BAC is ICAO optional (recommended) feature, in EU mandatory
- Interoperability issue
  - How to find out the passport is BAC-protected?

    → try & you find out

Alternative: Faraday Cage

- protects against unauthorised access, but not eavesdropping
  - used in US passports, initially *instead* of BAC

Active Authentication (AA)

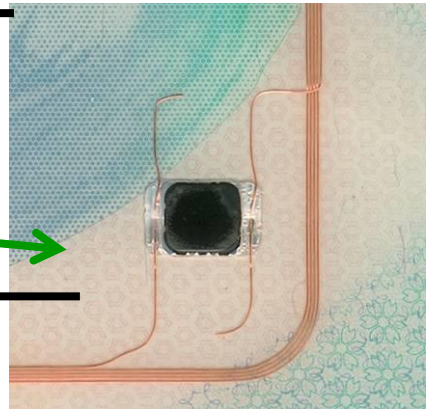
protects against passport cloning (which PA & BAC don‘t)

ie authentication of the passport chip,

using certificate & public key crypto in usual way

public key, signed by government (DG15)

send challenge c



sent response:

c encrypted with private key

Extended Access Control (EAC)

includes authentication of terminal by passport

- Why would we want this?

  Control access to privacy-sensitive information, namely fingerprints

- How would we do this?

  Some terminal certificate

  – ISO 7816 Card Verifiable (CV) certificates used rather than X.509 public key certificates.

- What are problems with this?

  Certificate revocation hard to realise

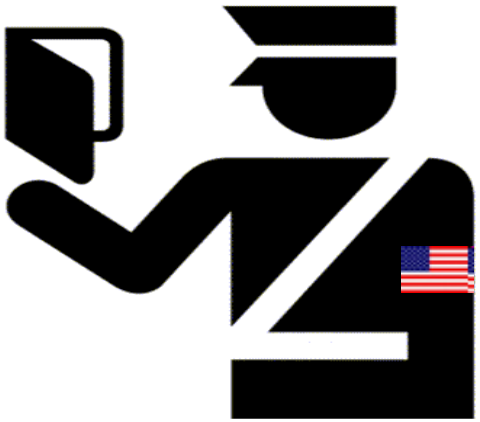
  – how do you revoke a terminal certificate on all passports?
    - you can't, so only certificates for short periods

  – passport does not have time to check certificate expiry
    - chip can only record date of last transaction

Extended Access Control (EAC)

1. certificate

preventing unauthorised reading of fingerprint info



2. fingerprint, please

3. prove you have access

4. certificate + proof

5. fingerprint

Extended Access Control (EAC)

Two phases

- Chip Authentication
  - replaces AA
  - starts Secure Messaging (SM) with stronger keys
- Terminal Authentication
  - uses traditional challenge-response:
  - terminal sends certificate chain to chip
  - chip sends challenge
  - terminal replies with signed challenge

Checking expiry of certificates by passport requires knowing the date.
Passport keep track of latest date in trusted certificates.

problems with passports,
so far...

Recall: passive vs active attacks on RFID

passive attacks

- eavesdropping on communication between passport & reader
- possible from several meters

active attacks

- unauthorised access to passport without owner's knowledge
- possible up to ≈25 cm
  - activating RFID tag requires powerful field!

- aka virtual pickpocketing
- variant: relay attack

Problem with BAC: low entropy in MRZ

- MRZ key based on passport number, expiry and birth dates
- passport numbers typically issued in sequence, so low entropy, and strongly correlated with expiry date
  - 3DES max 112bit, BAC max 56/74bit, in practice 30-50
- off-line brute force attack on eavesdropped traffic is possible [Marc Witteman & Harko Robroch, 2006]
- first discovered for Dutch passport, but other countries had the same problem
- solutions?
  - changing the key derivation procedure rejected by ICAO for compatibility issues
  - not handing out passport no's in sequence causes organisational & operational problems

Problems with Belgian passports

- First generation of Belgian passports (2004-2006) did not support BAC
  - so MRZ (DG1) skimmable in faction of a second, all passport info in about 10 secs
- These passports also provide info not required by ICAO, incl
  - place of birth
  - digital version of handwritten signature
- Also, same problem with low entropy of MRZ as Dutch passports

Problem with test version of Dutch passports

- Dutch passports contain a JavaCard JCOP chip, produced by NXP, which can also provide MIFARE Classic emulation
- Chips used in test-batch of the passport provided this MIFARE functionality, using default factory keys!
  - So Dutch public transport card or RU access card could be copied onto such chips
- In the real passport, MIFARE emulation was switched off…

Problem with ISO 14443: fixed UIDs

- Normal ISO 14443 tags sent a fixed UID as part of the anti-collision protocol
- This would allow tracking of individual passports

- Producing random UID requires non-standard hardware
- Some countries still used fixed UIDs (eg Italy)

- First batch of Dutch passports did not have truly random UIDs, as 2 bits in the random UIDs are always the same...

Problems with terminals

Some terminals crashed with buffer overflows on malformed JPEG: missing input validation, as usual...

Scan This Guy's E-Passport and Watch Your System Crash

By Kim Zetter 08.01.07

RFID expert Lukas Grunwald says e-passport readers are vulnerable to sabotage.
Photo: Courtesy of Kim Zetter

A German security researcher who demonstrated last year that he could clone the computer chip in an electronic passport has revealed additional vulnerabilities in the design of the new documents and the inspection systems used to read them.

Lukas Grunwald, an RFID expert who has served as an e-passport consultant to the German parliament, says the security flaws allow someone to seize and clone the fingerprint image stored on the biometric e-passport, and to create a specially coded chip that attacks e-passport readers that attempt to scan it.

Grunwald says he's succeeded in sabotaging two passport readers made by different vendors by cloning a passport chip, then modifying the JPEG2000 image file containing the passport photo. Reading the modified image crashed the readers, which suggests they could be vulnerable to a code-injection exploit that might, for example, reprogram

Problem: determining passport origin

- Error messages of the card reveal manufacturer
  - ie provide fingerprint

- BSc thesis by Henning Richter in Nijmegen

deVerdieping
Trouw

• Legio criminele toepassingen

Na ov-chip nu ook lek in paspoort

De chip in het nieuwe Nederlandse paspoort en andere passen is 'lek'. Dieven kunnen snel zien of iemand een paspoort bij zich heeft en uit welk land hij komt.

Vincent Dekker

Moderne paspoorten in tassen of binnenzakken verraden draadloos hun aanwezigheid én uit welk land ze komen. Onderzoekers van de Radboud Universiteit in Nijmegen hebben een beveiligingslek ontdekt in de chip die de pas juist veiliger moet maken.

„We hebben op de universiteit studenten van tien nationaliteiten en bij allen kunnen we ongezien zeggen uit welk land hun pas komt", aldus Erik Poll, die samen met Woi-

antwoorden op elke correcte vraag van een officieel leesapparaat, zoals bij de douane. Maar men is vergeten dat ook te regelen voor antwoorden op verkeerde vragen. In de praktijk blijkt dat elk land een eigen manier heeft bedacht om met foute codes om te gaan. Analyseer de foutmelding die je terugkrijgt na het bewust versturen van een verkeerde code en je weet uit welk land het paspoort komt."

Foutmeldingen verraden veel over de werking van computers en zijn al vaak gebruikt om systemen te kraken. Daar heeft de Icao echter niet genoeg bij stilgestaan, blijkt nu.

De chip in het paspoort werkt, net als die in bijvoorbeeld de gekraakte OV-chipkaart en toegangspasjes, met de draadloze rfid-technologie. Daardoor is een rfid-lezer van een paar tientjes genoeg om de paspoorten te herkennen. Om ze geschikt te

Olympische fakkelt San Francisco volge

Na Londen ontaardde ook in Parijs de olympische fakkeltocht door Tibetprotesten in chaos. De volgende steden maken hun borst al nat.

Van onze redactie buitenland

De olympische vlam verliet gisteravond Parijs, op weg naar de volgende bestemming: San Francisco. Maar sommige officials beginnen zich vanwege alle Tibetprotesten af te vragen of de estafettewel door moet gaan.

De route van de vlam door Parijs werd gisteren ingekort. De protesten tegen het Chinese ingrijpen in Tibet veroorzaakten dermate veel chaos dat de fakkel liefst vijfmaal gedoofd moest worden – volgens de organisatoren één keer vanwege een defect en vier keer uit voorzorg. De olympische vlam bleef volgens hen wel permanent branden in een busje. Maar de chaos werd zo groot dat de route moest worden verlegd en een bezoek aan het Parijse stadhuis helemaal werd afgeblazen.

Rond tien uur vertrok het vliegtuig uit Parijs. In San Francisco stonden de volgende demonstranten al klaar om de Chinese omgang met Tibet aan de kaak te stellen. Gisteren

Fingerprinting passports

- All e-passports react the same to *correct* protocol runs....
- but what about *incorrect* ones? Eg
  - commands out of sequence
    - eg B0 (READ BINARY) *before* completing BAC
  - commands not in the ICAO specs at all
    - eg 44 (REHABILITATE CHV)
  - commands with silly parameters

e-passport commands & responses

Commands sent to card include 1 instruction byte, eg

- A4 SELECT FILE
- B0 READ BINARY
- 84 GET CHALLENGE
- 82 EXTERNAL AUTHENTICATE
- ...

Responses from card include 2 bytes status word, eg

- 9000 No error
- 6D00 Instruction not supported
- 6986 Command Not Allowed
- 6700 Wrong Length
- ...

Defined in ISO7816, re-used in ICAO specs

Example responses to B0 instruction

B0 means "read binary", and is only allowed after BAC

	response (status word)	meaning
Belgian	6986	not allowed
Dutch	6982	security status not satisfied
French	6F00	no precise diagnosis
Italian	6D00	not supported
German	6700	wrong length

255 other instructions to try,
and we can try different parameters ...

Fingerprinting passports

- Response to strange inputs provides unique fingerprint for ten nationalities originally tested
  - Australian, Belgian, Dutch, French, German, Greek, Italian, Polish, Spanish, Swedish

  The fingerprints depends on implementation choices in the software

- 4 commands suffices to distinguish between these nationalities. The response to
  - instruction byte 82 identifies Australian, Belgian, French, and Greek
  - A4 identifies Dutch and Italian
  - 88 identifies Polish and Swedish
  - 82 with different parameter identifies German and Spanish

  Code to do this is very simple & very fast

The small print in the specs

"A MRTD chip that supports Basic Access Control *must* respond to unauthenticated read attempts with ‘Security Status not satisfied’ (6982)"

[PKI for machine readable travel documents offering ICC read-only access, version 1.1. Technical report, ICAO, Oct 2004.]

but what constitutes a "read attempt"?

Countermeasures to fingerprinting

- better specs
  - clearly prescribing standard error responses
  - or, all countries could simply use a common open source implementation
    - eg our Java Card implementation [http://jmrtd.sourceforge.net]

  but to late to do now, as many implementations already exist

- metal shielding in passport cover (Faraday cage)
  - defence-in-depth

Abuse cases for fingerprinting?

- Passport bomb triggered by a specific nationality
- Selection of potential victims by passport thieves

Fortunately, limited range for active attacks (25cm, maybe a bit more) reduces any serious threat

Also, there may be easier ways to detect nationality...

Passport bomb

http://www.youtube.com/watch?v=-XXaqraF7pI

What goes wrong in practice?

Technical things that go wrong: defects

Some real e-passports fail to meet the standard, eg

- Wrongly calculated hashes
- Encoding of certificate fields: printable string ↔ UTF8
- Wrong identifiers in certificates
- Printed MRZ data not matching the one stored in the chip
- Truncated photos

Some countries have warned others about passport batches they issued with known defects

Internationally, there are discussions about a standard format for defect lists to report defective batches

Organisational hassle: issuance

How reliable is the issuance process?

- Someone obtained a Dutch ID card with a picture of himself as the Joker from Batman

- Can staff at town halls take good fingerprints?

- Fingerprints are no longer checked when people collect passports, because of the numbers of false positives
  - false negatives rates always a few percent…

Organisational hassle: checking

- Few countries bother to read the chip on a regular basis
- Exchanging certificates, bilateraly via diplomatic post, is a big hassle!
- Hardly any countries use fingerprint data
  - is quality of fingerprints info really good enough ?
  - yet more certificate hassle, as terminal have to be equipped with a short-lived terminal certificate, one for every country
- Do personnel trust the chip, and can they interpret errors?
- Or was the real motivation
  Automated Border Control?

Conclusions

Questions

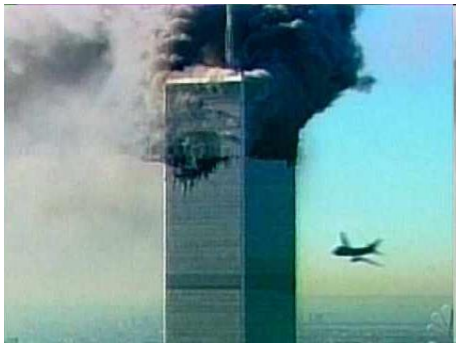
What is the problem solved/security improved by RFIDs in passports?

Advantages

+ Digital data in passport extremely hard to fake
+ Larger hi-res picture makes look-alike fraud harder

But

- Would it prevent another 9/11?
- Does it outweight the new risks & cost?
- Potential problem/opportunity: function creep?



Function creep

- Function creep: once a system is in place, its use of it will gradually be extended to other purposes
- After introduction of e-passport, Dutch goivernment proposed a national database with all fingerprints for police investigations
- Following discussions in parliament, this plan has been stopped – for now....

Other existing & future e-ID initiatives

- US Passport Cards and Enhanced Drivers' License (EDL) include a simple RFID tag, which just broadcasts a number
  - readable at larger distances than ISO14443 passport tags
- ISO18013 standard for e-driving license
  - very similar to ICAO specs
- Additional functionality for e-id cards: digital signatures
  - already in some national id cards in EU
- remote authentication: Active Authentication (AA) could be used over the internet

Questions?

- Code for passport terminal and passports available at http://jmrtd.sourceforge.net

- e-passport apps for Android NFC phones: NFC Passport Reader and eClown