

E-identity and Machine Readable Passports



Nicolas T. Courtois ¹, ex. 2

- ¹  - University College of London, UK
- ²  = [Axalto+Gemplus]
security to be free

Summary:

1. Goals of e-Passports
2. Discussion: Wired vs. Wireless
3. ICAO Specs
4. Security, Attacks
5. Second Generation

Electronic Passports Today!

- Chip integrated in the cover
 - Main goals: store biometric data [US congress]
 - Machine Readable Zone (**MRZ**)
 - Personal and biometric data (photo)
 - protected by basic access control (**BAC**)
 - Key = $f(\text{MRZ})$
 - **PA: Passive Authentication**: PKI, all data authenticated by a mandatory static signature,
 - Digital Signatures with RSA/DH, ECC or both
 - More advanced security mechanisms [new]
 - (optional) – Challenge-response **Active data Authentication (AA)**
 - Extra data [fingerprints]:
 - Access only by “authorized border authorities”
 - Extended Access Control (**EAC**) mechanism
- All EU passports >2009



E-identity: Introduction and Goals



Questions

- What are the functionalities of a Passport or Identity Card?
- Why adopt Machine-Readable Travel Documents = MRTD?



Old World...



A. Goals [old world]

Main security functionalities of an ID Card and/or passport:

1. Proves the existence of such a person (prevents forged identities).
 - Works well also with a photocopy (and used !).
2. Identification = Entity Authentication.
 - Possession (cf. 123 below).
 - Biometric information: photo, colour of eyes, height, fingerprint [US social security cards], ...
3. Message authentication possible: sign and compare signature. Used for bank cheques.
123. Access Control: total user control (don't lend it, wait behind the line).



But Securities Can Always Be Circumvented

<http://www.guardian.co.uk/terrorism/story/0,,2038442,00.html> [March 2007]

In the UK, according to the Home Office minister:

- 16,500 fraudulent passport applications received / year
 - Less than half of fraudulent applications are detected (!)
 - About 10 000 per year FALSE passports (0.5%)
were issued by UK Home Office Identity and Passport Service
 - Example: Dhiren Barot, the most senior al-Qaida terrorist ever captured in Britain received two British passports under TWO different FRAUDULENT identities.
- Now new passport applicants in the UK will be interviewed.
- They will ask them questions for which the answer is known (from various databases):
 - where and when their parents were born
 - which bank accounts they hold
 - who lives with them,
 - whether they have a mortgage,
 - etc

LOW TECH
ATTACKS!





New World...



A. Same Goals

Main security functionalities of an ID Card and/or passport:

1. **Proves the existence** of such a person (prevents forged identities).
 - Works well also with a photocopy (and used !).
2. **Identification** = Entity Authentication.
 - Possession (cf. 123 below).
 - Biometric information: photo, colour of eyes, height, fingerprint [US social security cards], ...
3. **Message authentication** possible: sign and compare signature. Used for bank cheques.
123. **Access Control**: total user control (don't lend it, wait behind the line).





B. Take it Further



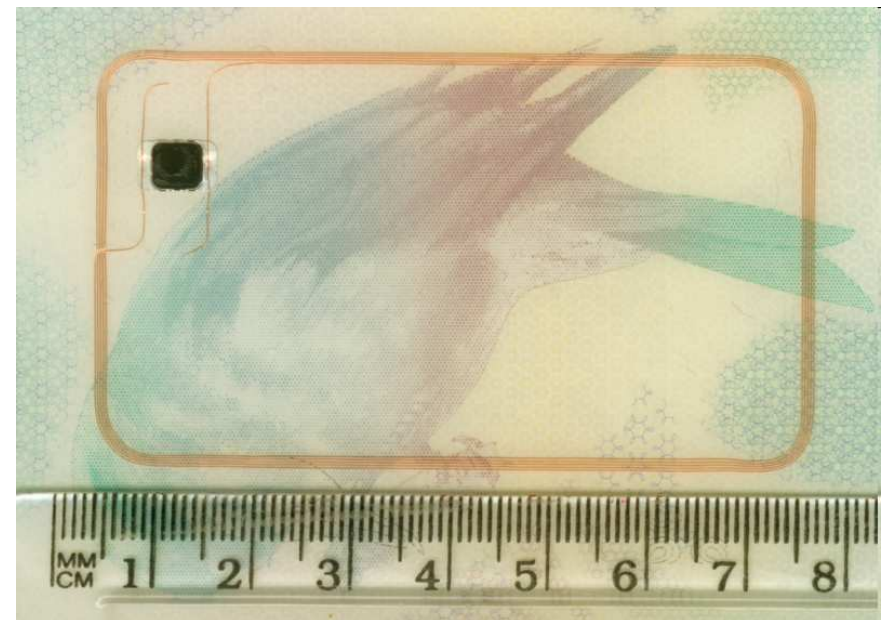
So far: Humans verify the authenticity...

- Compare (really ?) photos/signatures.
- Get rid of the humans:
 - Reduce cost [financial / right-wing reason]
 - More convenience for existing employees [trade-union friendly version] and passenger convenience [right-wing].
 - Are the weakest link [security motto].
Not 100 % reliable, unequivocal identification needed (possible ? not in 2010).

B'. Towards E-passports / E-Id

Embed a chip in the cover.

- Large loop antenna
- Sign



B'. Towards E-passports / E-Id

Humans Lose to Machines.

E-identity - A chip card / contactless allows:

- To store more/better biometric data.
- Much stronger authentication (!):
 - can sign systematically with a PK signature (better than PK-authentication, can certify entry to a country). Exists: fill a form and sign, but not used so far just to prove identity.
- Create police state,
- Steal and re-sell people's privacy.
- Sell more smart cards [Gemalto].
- More frequently used, new applications, virtual economy enabler.



A+B' = Old Goals, New Solutions

The same main functionalities of an ID Card and/or passport:

1. Proves the existence of such a person (prevents forged identities). Can be achieved with chip and electronic signatures [Static Signature, memory card needed].
 - Works well also with a photocopy ? POSSIBLE, short signatures, Quartz, HFE patent [Axalto].
2. Identification = Entity Authentication.
 - Possession
 - Biometric information – embedded in a chip, higher res.
3. Message authentication possible:
 - Automatic - sign “I was here”.
 - User-controlled - digitally signing documents.
123. Access Control: (shielding ?) escapes the user, smart card needed (RFID), cryptography needed.

Identity Cards with Chips



US

US “Passport Cards” and “Enhanced Driver License” (EDL)

- a low-end RFID tag:
 - broadcasts a unique UID
 - readable at large distance

Belgium – known as BelPIC



BelPIC:
>10 M since
2002-2003



BelPIC as an ID

5 files are publicly readable (need to insert the card):

- the ID data,
- the address (not printed on the outside of the card anymore),
- the citizen's black&white picture,
- +two government certificates to verify the integrity and authenticity of the three citizen-related files

BelPIC as PKI

1. One authentication public/private key pair with certificate:
 - Allowing a citizen to authenticate him/herself using the card and PIN in on-line situations.
2. One digital signature public/private key pair with certificate:
 - allowing to digitally sign forms, documents, etc. using the card and PIN in on-line and off-line situations.
 - This signature has the same legal value as the citizen's handwritten signature.
3. Two certificates (Citizen CA and RootCA) allowing the verification of the citizen public keys.

BelPIC - Applications

No restrictions, can and is used for anything.

- On-line income tax declaration
- Electronic registered letter application
- On-line banking based on eID authentication
- Access to container parks (in every municipality) based on eID card
- On-line car license plate request
- Integration with the social security card
- On-line request of birth certificates and other documents through city website
- Physical building access
- Etc.

Estonia



Allows to vote over the Internet! [October 2005]

Portugal [2008-2011]

www.Cartaodocidadao.pt , 2007: pilot in Açores,

10 Mu will be rolled-out

A common access portal: Internet or phone.

Functionalities:

- Identification of the holder
- Authentication of the chip
- Digital Signature & OTP
- Biometric data storage: optional



UK [2008-]

RFID capable!

2008: Foreign Nationals Only (for now)



SOURCE: UK Border Agency

E-Driving Licence

ISO 18013, very similar to ICAO e-passport specs.



Short History of e-Passports



Some Facts to Start...

- Started in 1998 in Malaysia:
 - 5 M E-passports in circulation in Malaysia. Thumb fingerprints.
- 2005: US congress:
 - All [Visa Waiver Program: 27, most EU] passports emitted after October 2005 have to carry biometric information (!!). (at least face recognition, optional: fingerprint, iris)
- 2005: all US passports have chips.

Privacy issues with e-Id:

Id. Attacks on Identity: **Old.**

forgery, impersonation, etc...

- Chip cards: security as good as with paper Ids.
- **Contactless: substantially weaker !**



C. Confidentiality = Privacy + Anonymity: **Hot issue !**

- Chip cards: -(w.r.t. 3rd party attackers:) sometimes even less problems than with classical Ids ! –but much easier tracking, data-gathering etc..
- **Contactless: great danger !**

⇒ Main problem: access control (large meaning).
The US government decided to use **contactless** !



Worse than That

- For a long time the Bush administration wanted to deploy e-passports without any confidentiality protection
 - everybody could read your biometric data,
 - even unnoticed
 - technically speaking: no BAC, we explain BAC later
 - later they claimed that the passport cover that would shield the chip will be enough security.
 - but it wasn't very secure still.
- Many famous US professors and activists fought against this project
 - They partly won

Bruce Schneier vs. Bush Admin

The most respected security expert says:

« ...Since 9/11, the Justice Department has asked for, and largely received, additional powers that allow it to perform an unprecedented amount of surveillance of American citizens and visitors... »

« ...the "**Big Brother is Watching You**" style of total surveillance is slowly becoming a reality... »

[Bruce Schneier: « Toward Universal Surveillance, CNET.com and Cryptogram.]

« ...**People** living in this kind of society **are not free**, despite any illusionary security they receive. It's **contrary to** all the **ideals** that went into founding **the United States**... »

[Bruce Schneier, Identification and Security, SF Chronicle and Cryptogram.]



Schneier on Chip vs. Contactless:

Security is always a **trade-off**. If the benefits of RFID outweigh the risks, then maybe it's worth it.



But there isn't.

There's **a large cost** in security and privacy, and **no benefit**.

[Bruce Schneier: Cryptogram October 2004.]



Schneier on Electronic Passports

- « ... Unfortunately, RFID chips can be read by any reader, not just the ones at passport control... »
- « ...The administration claims that the chips can only be read from a few centimeters away, so there's no potential for abuse. This is a **spectacularly naive** claim. All wireless protocols can work at much longer ranges than specified. In tests, RFID chips have been read by receivers 20 ^(incorrect???) meters away. Improvements in technology are inevitable... »
- «... The administration is deliberately choosing **a less secure technology without justification**... »

[Bruce Schneier: Cryptogram October 2004.]



Schneier Says It:

« It's the only reason I can think of for the administration wanting RFID chips in passports: they want surreptitious access themselves. **They want to be able to identify people in crowds. They want to pick out the Americans, and pick out the foreigners.** They want to do the very thing that they insist, despite demonstrations to the contrary, can't be done.

Normally I am very careful before I ascribe such sinister motives to a government agency. Incompetence is the norm, and malevolence is much rarer. But this seems like a clear case of the government putting its own interests above the security and privacy of its citizens, and then **lying** about it. «

[Bruce Schneier: Cryptogram October 2004.]



Wagner Paper [highly influential]

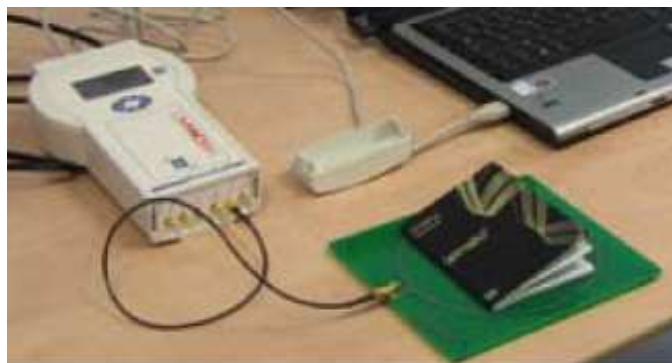
[Juels, Molnar, Wagner], eprint.iacr.org, April 2005.

1. Page 7: the public key should be linked to the specific passport => ICAO specified that Active Authentication done together with MRZ read.
2. Page 10: the US government uses Active Authentication => must implement MRZ reader.
3. THEN, Basic Access Control is free, no cost.
=> “reasons cited”... “are not convincing”.

These (and many other) voices forced the
US government to adopt BAC.



RFID



Crucial Vocabulary Problem



RFID Tags - equivalent to barcode or a memory card with no other security functionalities.



- Adopted by Wal-Mart (**as cheap as possible**) read data / kill command, ISO18000.
- **contactless smart cards** - writeable memory, microcontroller, crypto and security mechanisms, tamper-resistance.
 - ISO 14443 (13.56 MHz, <10 cm).
(eavesdropping – 5..25 m and much more: relay, military technology...)

Crucial Vocabulary Problem

We need to **COMBAT**
this vocabulary !

COMBAT cheap **RFIDs**
(equivalent to barcode with no security).

Much more than an electronic tag is needed !
Instead insist on:

- Full-fledged **contactless smart cards** with **crypto** and **tamper-proof** security.
- Much more added value. RFID \neq high-tech.
- Press \Rightarrow Gemalto stock price !!!



The Trouble with RFID Passports/ID



Some Shortcut Notations in my Slides

Id. Refers to attacks on **Identity**:
forgery, impersonation, etc...
=> important for the government



C. Refers to attacks on **confidentiality**
= **Privacy + Anonymity**.
=> important for the people



Recall Also:

[security] functionalities of an ID/passport:

1. Proves the existence of a person / passport /data
2. Identification = Entity Authentication.
3. Message authentication.

New Solutions => New Problems



- Goal 1 (out of 123):

1. Proves the existence.

=> Static Signature.

- works also with a photocopy
=> printed short signatures (cf. HFE patent).

Problems:

Id. Easy to copy if not protected.

C. Anonymity hard to achieve
(e.g; Name used for verification).



New Solutions => New Problems

2. Identification = Entity Authentication.

- Possession

Problems:

- With chip card OK.
- With contactless –

Id. “Possession verification” security still exists ?

- Yes with good shielding “Faraday cage”, **will be removed ???**
- Otherwise **No**, can be relayed, the passport is 1000 km from here...

C. Anonymity:

- non-existent if possession publicly verifiable,
- otherwise still in great danger.





New Solutions => New Problems

2. Identification = Entity Authentication.

- Possession
- Biometric information – embedded in a chip.

Problems:

I. Much easier to copy and re-use.



C. Contact-less: Much lower privacy/anonymity/security of a person.

- E.g. reuse biometric data.





New Solutions => New Problems

3. Message authentication possible:

- Automatic - sign “I was here”.
- User-controlled - digitally signing documents.

Problems:

Id. Copy / interception – not always a problem.

C. If publicly verifiable and contactless, bad security/privacy/anonymity.

⇒ Public key is secret [as in EMV] – illusion.

⇒ “Designated verifier” techniques ?!

Axalto Corporate Presentation [2005]



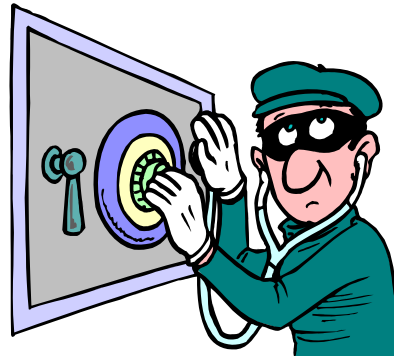
**Looks like a
plea against
contactless !!!**

(privacy is HARDer to
achieve with
contactless chips...)

- Your virtual identity stays with you
- You provide your credentials only when you want, protecting your privacy



Low-Tech Attacks on RFID Passports/ID



List of Attacks (1)



- Clandestine scanning – leakage of private data, fraud, ...
 - Starting point to identity theft (massive plague in US).
- Clandestine tracking – people in a city...
 - Hot-listing: building databases, link UID to a face (later),
- Eavesdropping on legitimate transaction (airport) – CANNOT be prevented by shielding (Faraday cage).
 - “Function creep”: shops/banks present at airports can spy on people.
 - Passive, much large distance.
 - Impossible to detect.
- Relaying complete transactions (different airport, biometric systems have big tolerance !).

List of Attacks (2)



Passport photo: NOT PUBLIC, good quality, specific conditions: hard to find !!!

Attacks:

- Leakage and Re-use of biometric data: reused in other automatic systems
 - Matsumoto's gummy fingers => PC authentication, corporate access etc,
 - holding a photo – works [Adler] !)
 - => Gemplus: Naccache-Coron-Barral BioEasy^R solution [not perfect]
- Cryptographic weaknesses: e.g. ICAO spec:
 - MRZ gives remote access to the passport for eternity...

Later:

- Finding a biometric Twin.
- Challenge semantics attack.

RF Eavesdropping

Contact-less ISO 14443 - Power

Typical working range: 0-5 cm, possibly 10 cm.

- Power it up:

Near-field communication:

$$P \sim D^3$$

At 13.56 MHz:

0.5 m => 500 W to power the passport.

5 m => 0.5 MW ! One could kill people and electronic devices with that...



ISO 14443 Eavesdropping

2. Eavesdrop the card:

- SNR 5-12 dB required =>
distance ≤ 0.8 m
 - (Schneier said 20 m, Riscure says <5 m)
- **IN FACT carrier detection** was demonstrated at 20 m: lose information => gains distance, Shannon's laws.

3. Eavesdrop the reader: 25 m is considered to be the maximum.

Contact-less – a difference ?

Wireless vs. wires (lack of physical link):



- For passive attacks (eavesdrop):
 - only qualitative difference, we can also spy on a cable and this remotely through radiation!
- For active attacks:
 - MUCH more power to the attacker.
 - Man in the middle attacks, relay attacks.



Privacy:

- Individuals
- Country of Origin

Contactless – Privacy

Three levels:

1. Recognize/track individuals (for example entering a shop, large antenna).
2. Recognise a US citizen
 - for example make a bomb that explodes if a US citizen is within 30 cm
3. Target anybody that has an RFID chip
 - (isolated country such as North Korea, anti-RFID activist etc..)

Elements that will Betray Your Passport..

- UID
- Answers to non-standard commands
- ATR/ATS



Here come the details...



UID

Anti-collision mechanisms:

- when two chips are within the range of the reader, allows nevertheless to talk to one of them (a very good reader can even access each card, see Oyster card reader in London underground).

ISO 14443 anti-collision use unique chip identifiers UID that is:

- ?
- fixed with some issuers,
 - random with others (recommended by ICAO)
 - Our French passports, random UID
(2006: starts with '08', not 2008 one)

> 26
< 04 00
> 93 20
< 08 D9 B3 14 76
> 93 70 08 D9 B3 14 76 || CRC
< 20 || CRC

=> UID : 08 D9 B3 14



ATR

- ATR:
 - In fact computed by the reader from the ATS (Answer to Select).
 - Contains “historical bytes” that identify the card and OS version, and allow to recognise the chip by its ATR)

Differences in Implementation

- Even without BAC we can communicate with the chip
 - We cannot read the data groups
- The differences in implementations allow easily guess the issuing country (!)

Eric Poll [Nijmegen] Attacks

Small print in the spec:

"A MRTD chip that supports BAC must respond to unauthenticated read attempts (including selection of (protected) field in the LDS) 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.]

Most developers ignored this...

Eric Poll [Nijmegen] Attacks

Send various ISO commands, observe the error messages:

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

Eric Poll [Nijmegen] Attacks

One can quickly and UNIQUELY identify the following passports:

- Australian, Belgian, Dutch, French, German, Greek, Italian, Polish, Spanish, Swedish

These use exactly the same chip, cannot tell apart:

- Dutch, Irish, Finnish and Slovak

Reliability, DOS Attacks

Problems

The passports used to last 10 years, now only 5 years.

- One can by accident damage the chip:
 - For example put in the micro-oven.
- It is possible to jam 13.56 MHz transmission
- Lucas Grunwald, German security expert, found a buffer overflow attack against two ePassport readers made by different manufacturers:
 - he copied the content of a passport, modified the JPEG2000 face picture, and wrote the modified data in a writable chip.
 - the reader crashed.

Defences



Shielding

- Faraday Cage
 - Protects from RF access
 - Gives the user full control
- back again



£12.75



£2.54

BTW. Apparently included in the cover of some passports, which?



New Solutions => Main Problem

123. Access Control

⇒ Good **shielding** – almost OK, few attacks...
will probably not be done, still remain:



Legal and Political Questions

- ⇒ Work / debate on who and under what conditions should access the chip data and functionalities.
 - ⇒ Need for advanced crypto solutions to implement whatever the bilateral agreements between governments and state laws will decide...

Contactless – security harder but possible

The US government decided to use
contactless !



- It will be **hard** to achieve good security then...
 - Not simple **RFID**s (barcode / simple storage).
 - Full-fledged **contactless smart cards**
- There is no fundamental problem,
 - crypto + secure hardware can solve it ?!?
 - **access control** needed.
 - who profits from this highly political debate ? The industry.

ICAO 9303 Standard



ICAO
/,aɪ,keɪ'ou/

<www.icao.int>

International Civil Aviation Organisation

U.N. specialized agency,

- established 1944
- aviation safety & security



ICAO 9303, 6th Edition System



Based on mainstream standards:

- ISO7816-X
- ISO 14443

Entities:

A. Issuer:

- State printing house, embassy, local authorities etc.

B. Contact-less chip embedded in the cover

C. Terminal, called “inspection system”.



A+B' = Old Goals, ICAO Solutions

The same main functionalities:

1. Proves the existence of such a person (prevents forged identities). **Passive Authentication. Mandatory.**
 - Works well also with a photocopy... **No proposal.**
 2. Identification = Entity Authentication.
 - Possession
 - Biometric information – embedded in a chip. **Mandatory.**
 - **Active Authentication (of the card). New functionality.**
 3. Message authentication (optional)
 - Automatic - sign “I was here” possible. ←
 - User-controlled digital signature. - **No proposal.**
123. **Access Control – “New” functionality. 2 Levels.**
(both) optional

Data in e-Passports



Memory

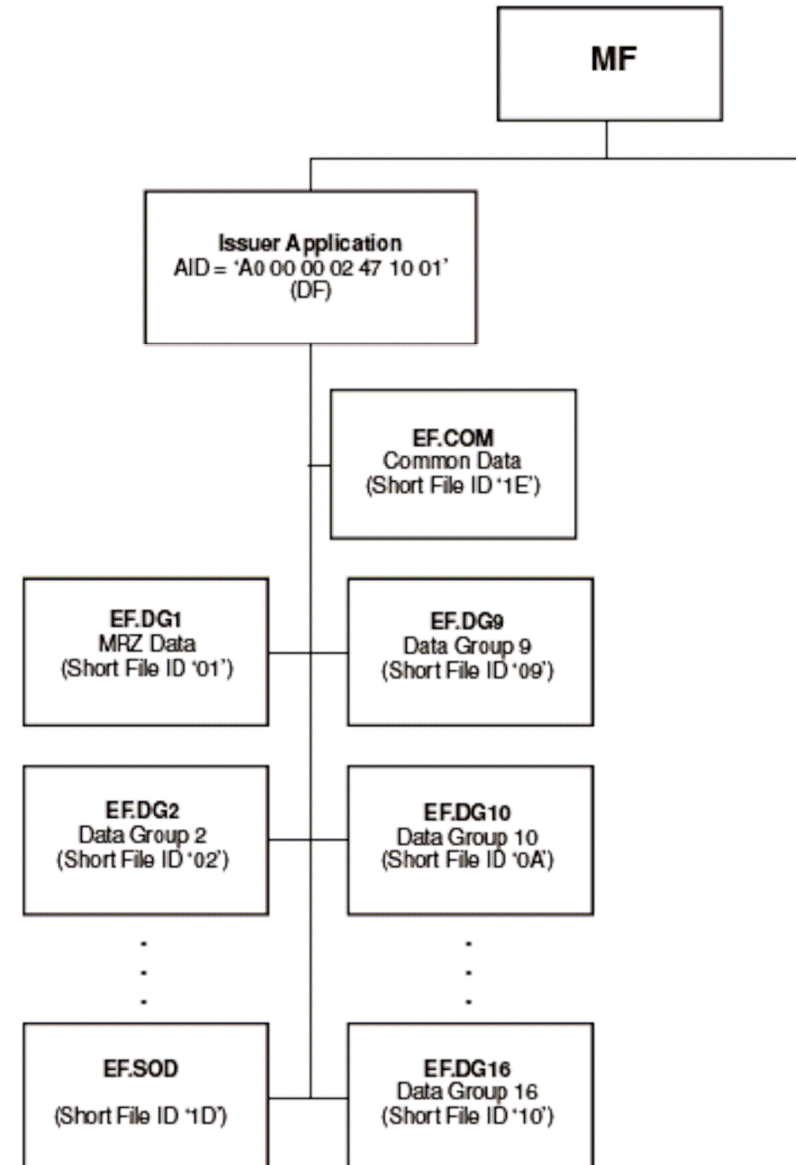
ICAO: requires 32 K
E²PROM minimum.

Typically 64-128 K.

Data in e-Passports

Many EFs (Elementary Files), all in one directory (DF)

- 16 data groups (DG)
 - EF.DG1 etc.
 - 2 data groups mandatory (DG1=MRZ and DG2=photo)
- EF.COM contains the version info and the list of present DGs
- EF.SOD contains the digitally signed list of hashes of DGs (static signature, a.k.a. PA)



All are Read only

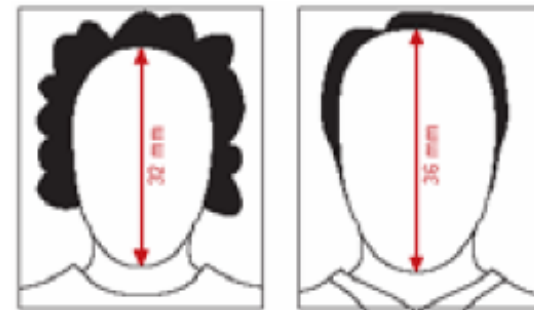


Data Quality

New requirements for pictures

- Photo booths
=> professional photographers

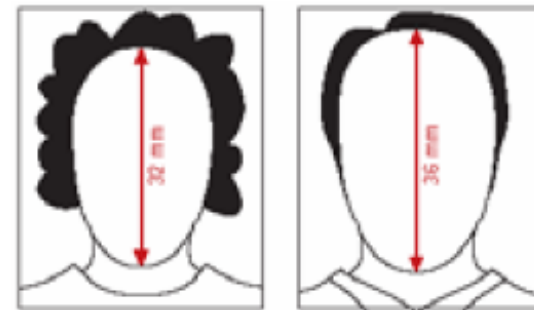
The rejection rate is now about 5%.



Norms for Photos (DG2)

Facial image (ISO 19794-5)

- JPEG or JPEG2000 image
- Basic, Full Frontal, Token Image
- Feature points (e.g. eyes)



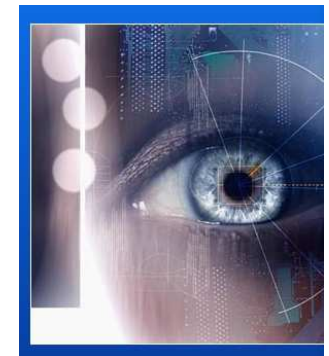
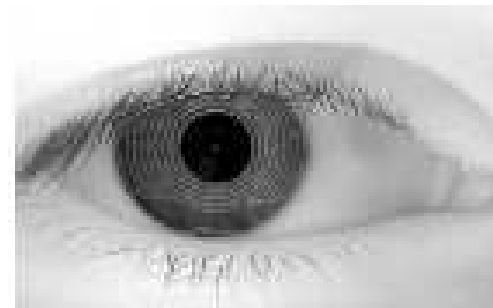
Norms for Fingerprints And Iris (DG3,DG4)

Fingerprint: ISO 19794-1

- Uncompressed
- WSQ, PNG, JPEG or JPEG2000



Iris image: ISO 19794-6



The Need for Access Control

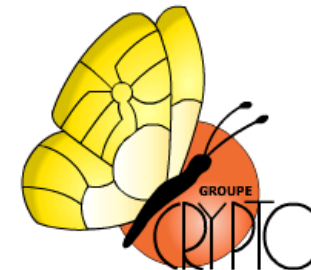


Le passeport biométrique belge recalé au BAC...

Vos informations personnelles sont en danger !

Gildas Avoine, Kassem Kalach et Jean-Jacques Quisquater

UCL Crypto Group, Louvain-la-Neuve, Belgique



Skimming Belgian e-Passports

Avoine, Kalach, and Quisquater:
showed that Belgian passports issued between
end 2004 and July 2006 do not include any
security mechanism to protect the personal data.

- these passports are valid until 2011.
- politicians just lied to the parliament:
 - Karel De Gucht, the Minister for Foreign Affairs, declared in the Parliament on 9th January 2007, after having been interpellated by MPs Joseph Arens and Jean-Claude Maene: "(...) the data embedded in the chip [of the Belgian passport] are protected by two security means: Basic Access Control and Active Authentication"
 - true only for passports issued after July 2006

Skimming Belgian e-Passports

Sitting next to you in a train, airport etc.



Le passeport biométrique belge recalé au BAC...

Vos informations personnelles sont en danger !

Gildas Avoine, Kassem Kalach et Jean-Jacques Quisquater

UCL Crypto Group, Louvain-la-Neuve, Belgique

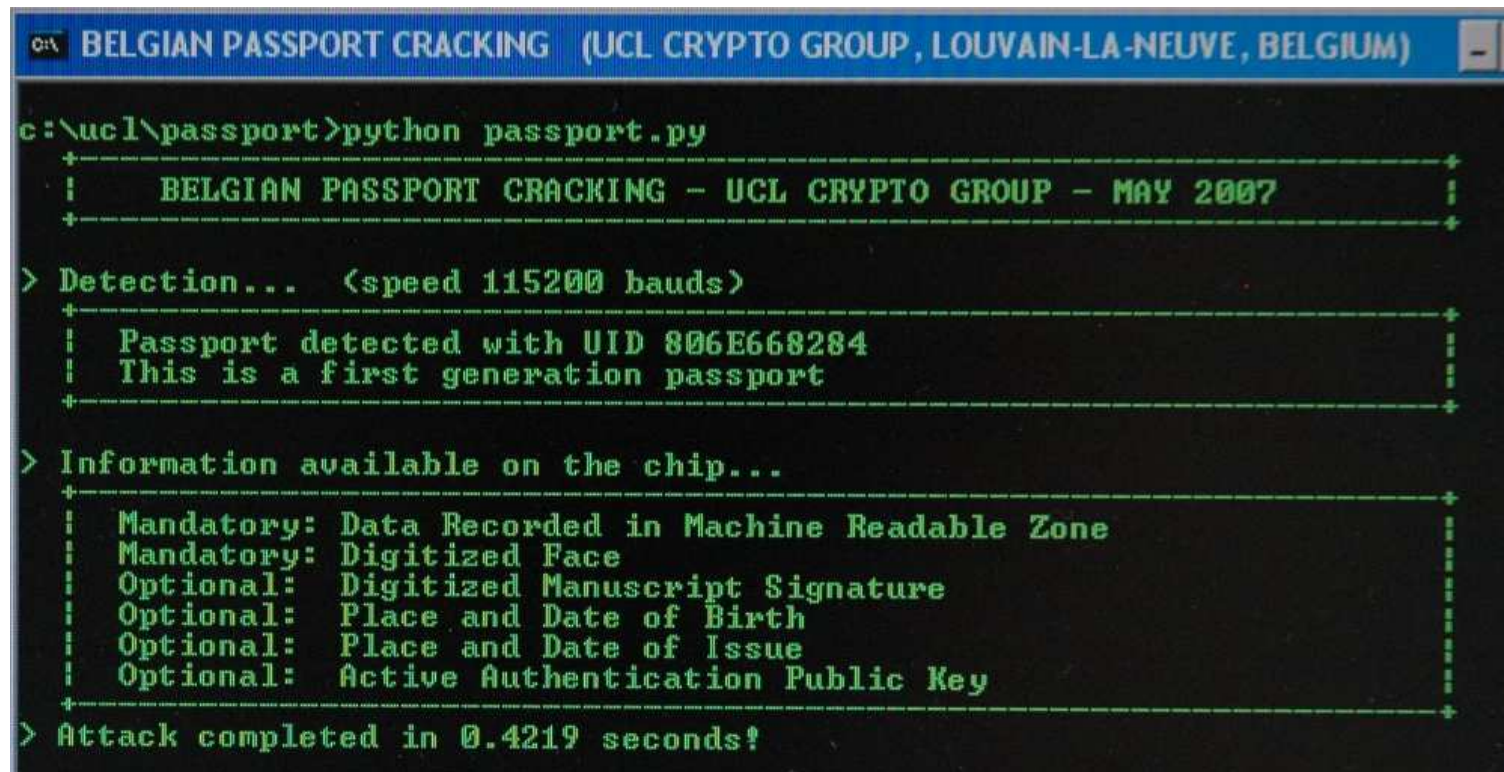


Skimming Belgian e-Passports

Issued between end 2004 and July 2006, no security

Everybody can read

[ALL OPTIONAL DATA WERE PRESENT]:



```

C:\ BELGIAN PASSPORT CRACKING (UCL CRYPTO GROUP, LOUVAIN-LA-NEUVE, BELGIUM)

c:\ucl\passport>python passport.py
+-----+
| BELGIAN PASSPORT CRACKING - UCL CRYPTO GROUP - MAY 2007 |
+-----+

> Detection... (speed 115200 bauds)
+-----+
| Passport detected with UID 806E668284 |
| This is a first generation passport |
+-----+

> Information available on the chip...
+-----+
| Mandatory: Data Recorded in Machine Readable Zone |
| Mandatory: Digitized Face |
| Optional: Digitized Manuscript Signature |
| Optional: Place and Date of Birth |
| Optional: Place and Date of Issue |
| Optional: Active Authentication Public Key |
+-----+

> Attack completed in 0.4219 seconds!
```

Access Control (SK mechanisms)



Access Control – 2 levels - scope.

- **Basic Access Control**, For facial image, and other data that “is possible to acquire from other sources” (e.g digital camera).

Initially optional BUT required for “global interoperable border crossing” => became de facto mandatory, everybody uses it now



- **Extended Access Control**, **optional**.

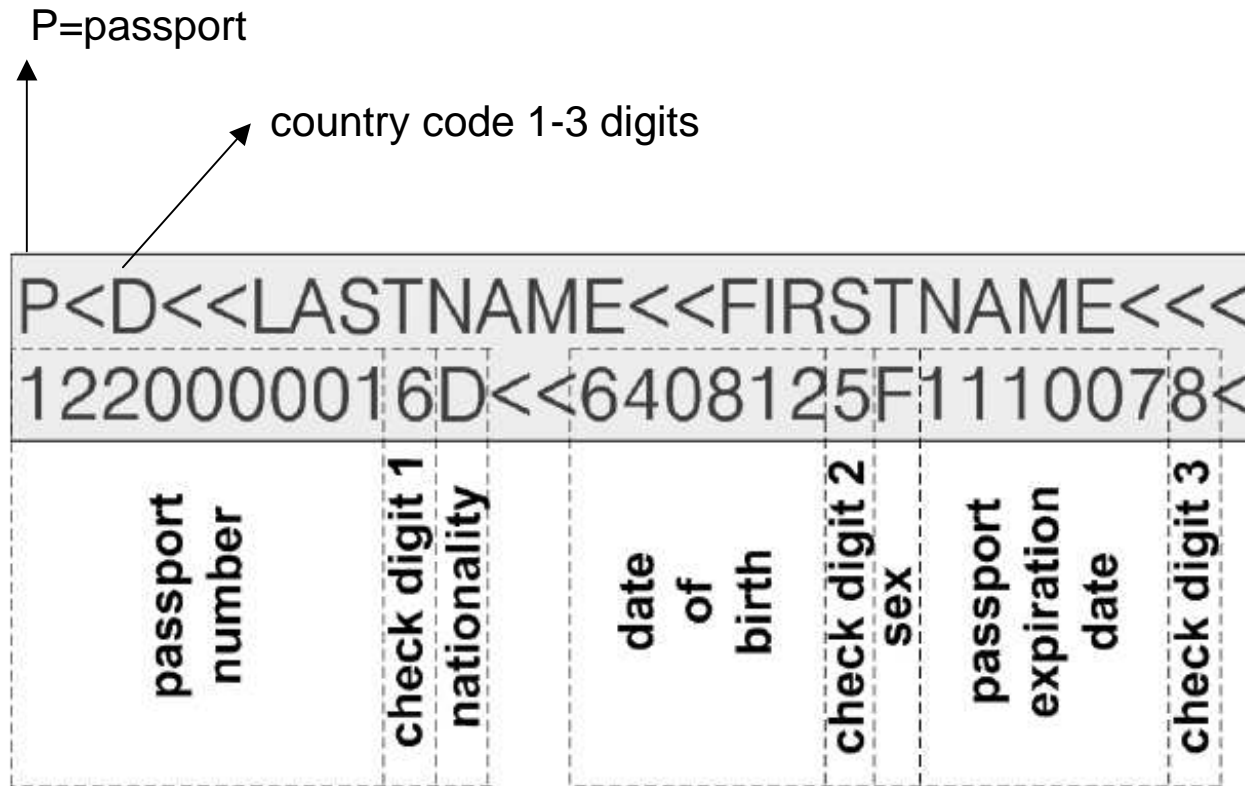
For fingerprints and other data that does not exist on passports for now, for verification by and “authorized inspection system”, that has to prove his identity to the passport... Initially not specified by ICAO - German BSI proposal.

The MRZ





MRZ Coding





Check Digit Algo (used 3 times)

1. encode:

< 0 1 2.. 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 0 0 1 2... 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35

2. multiply:

7 3 1 7 3 1 ...

3. add modulo 10:

Example “A2B” =>

$$10*7+2*3+11*1 = 87 = 7 \text{ mod } 10$$

**Why MRZ is also inside the chip?

Duplication?

Yes/No.

- security role of check digits – prevent non-intentional modification
- but **with DG1, these data are digitally signed!**



BAC: Basic Access Control

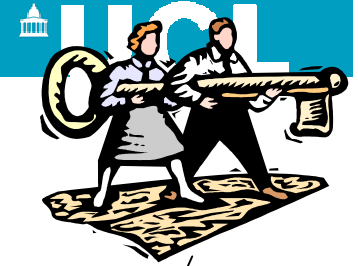
Basic Access Control by ICAO

- The terminal needs to have physical access to the MRZ.
 - MRZ is not accessible in chip.

MRZ:

- Passport number (9 chars typically)
- Date of birth
- Expiration date
- 3 check digits (simple CRC)



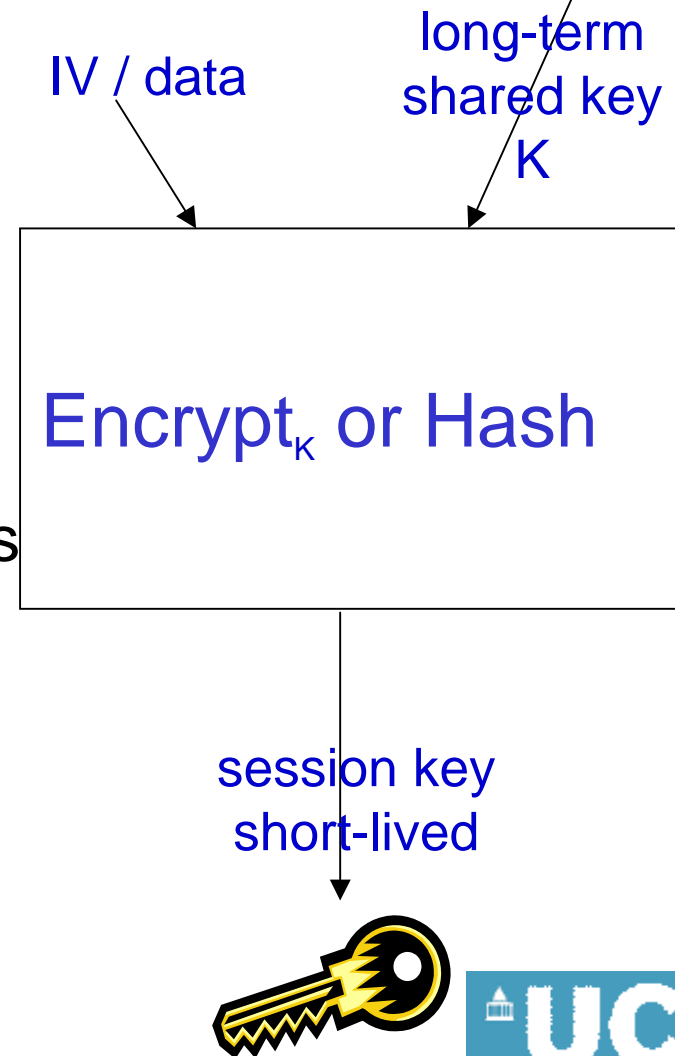


*Symmetric Key Derivation

Needed even if the key is already shared.

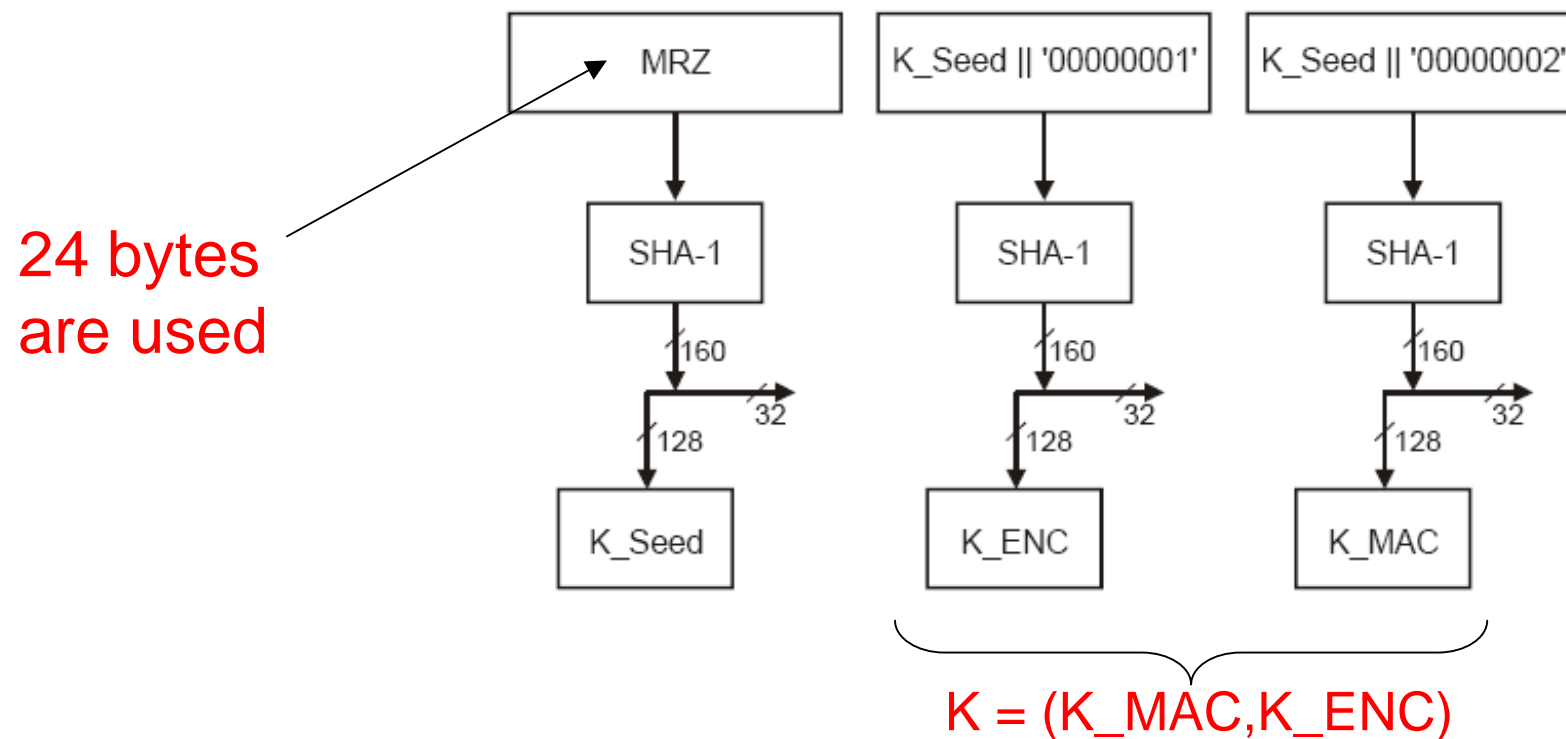
key diversification = key derivation,
very widely used in the industry:

- bank cards
- car locks
- contactless cards [e.g. Oyster]
- built-in component in stream ciphers
- etc.



BAC – Stage 1

MRZ => SHA-1 truncated to 128 bits =>
=> Then key derivation function following CWA-14890-1



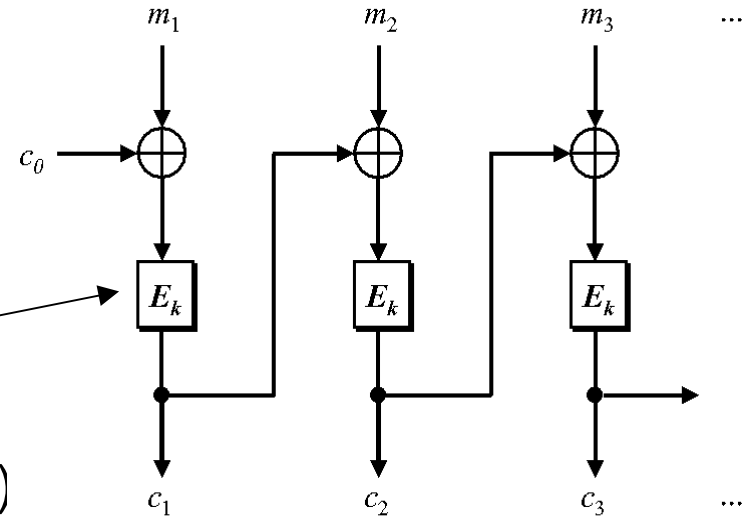
BAC – Stage 2

$K = (K_MAC, K_ENC)$, both are used =

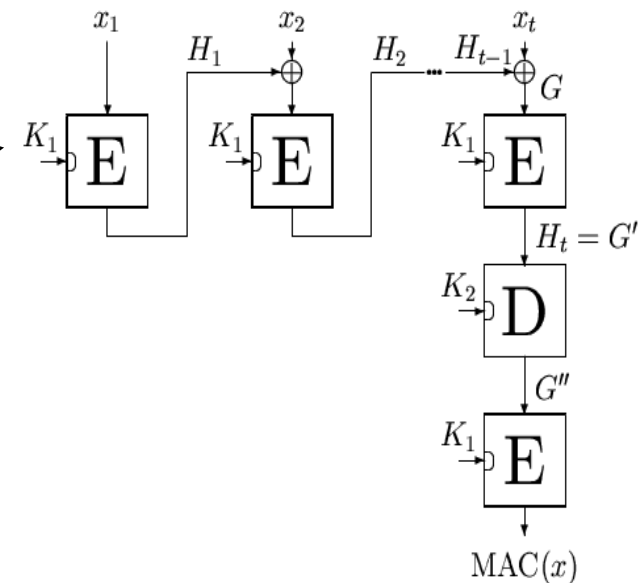
EA = **A**uthenticated **E**ncryption
= Encrypt + transmit a MAC

Both based on 3-DES:

- **E**: 3-DES in CBC mode with K_ENC
 - FIPS 46-3, ISO 11568-2, ISO 9797-1 (CBC-MAC, 3-DES, padding mode 2)

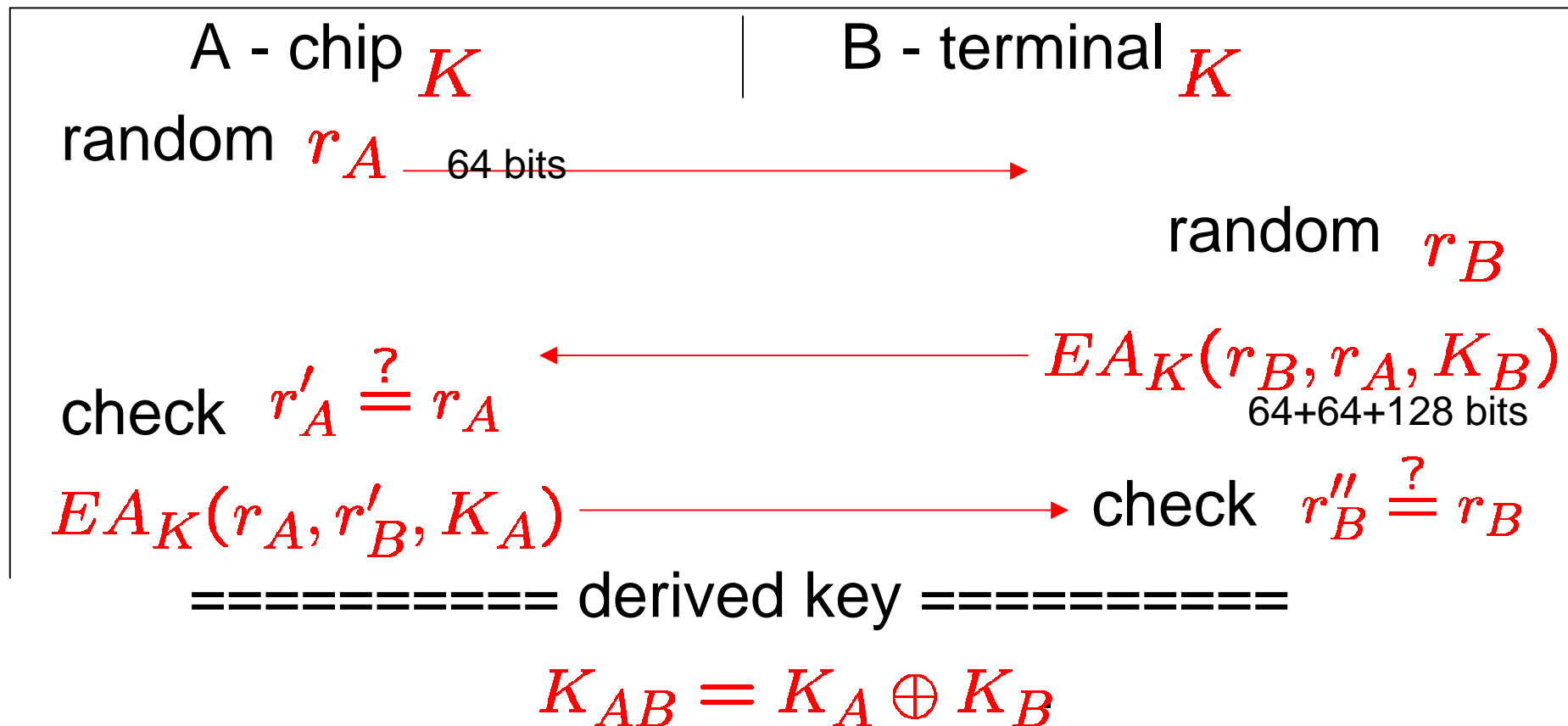


- **A**: DES + “Retail MAC” with K_MAC
 - FIPS 46-3, ISO 9797 (MAC algorithm 3, with output transformation 3, without truncation, block cipher DES, zero IV 8 bytes, padding mode 2).



BAC – Stage 3

- uses ISO 11770-2 symmetric key establishment mechanism.



BAC – Stage 4

===== derived key =====
 $K_{AB} = K_A \oplus K_B$

K_A and K_B are 128-bit keys generated at random by the card and the terminal.

K_{AB} => Used to encrypt all the
communications from now on...
(secure messaging).

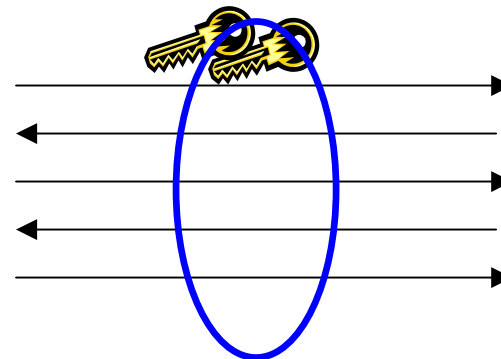
How Secure is BAC?



BAC

Meant to protect against:

- unauthorised R/W access to data
- eavesdropping
- altering the communication



encrypted and authenticated

Basic Access Control by ICAO

- Problem 1:

The resulting key has relatively **low entropy***

- dictionary attacks possible...

=>offline

Thus, **exhaustive search** to obtain the authentication key from a recorder eavesdropped session (offline **attack**) is possible - Big Brother is here,

attack remains costly, but not for the NSA.

- Wagner: US passport – 52 bits. Breakable by amateurs.

*[Two versions of dictionary attacks: break one given -**entropy**,
one out of many - **min-entropy**]

Entropy of the key << 112 bits

Depends on the type of document.

Best case: 10-year passports => breakable !

Contains:

- Document Number
 - Either a numeric Document Number,
 $365^{2*10^{12}}$ possibilities $\approx 2^{56.9}$.
 - Or an alphanumeric Document Number (used in practice ?),
 $365^{2*36^9*10^3}$ possibilities $\approx 2^{73.5}$.
 - More secure if chosen at random, but alphanumeric ? - will probably NEVER be chosen at random ? thus probably **always breakable** for offline eavesdropping attackers as above...
- Date of Birth (DoB) – 11-15 bits of entropy only (not-uniform).
- Date of Expiry (DoE) – low entropy (max 11 bits)

Entropy of the key $\ll 112$ bits

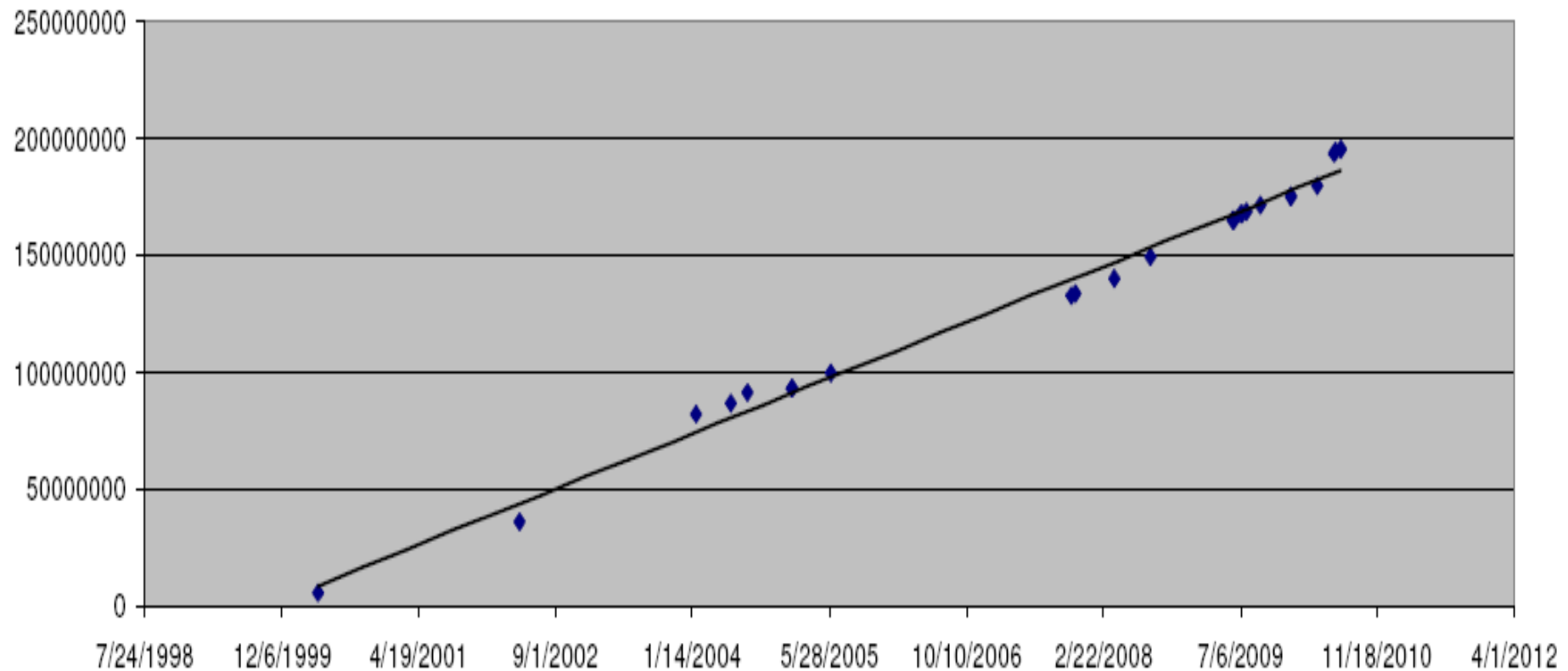
Still lower if attacker can correlate numbers and dates of expiry.

Entropy of the key - Netherlands

[...] *Predictability & dependency reduce entropy to 35 bits [..]*

Regular increase by about 50000 per day

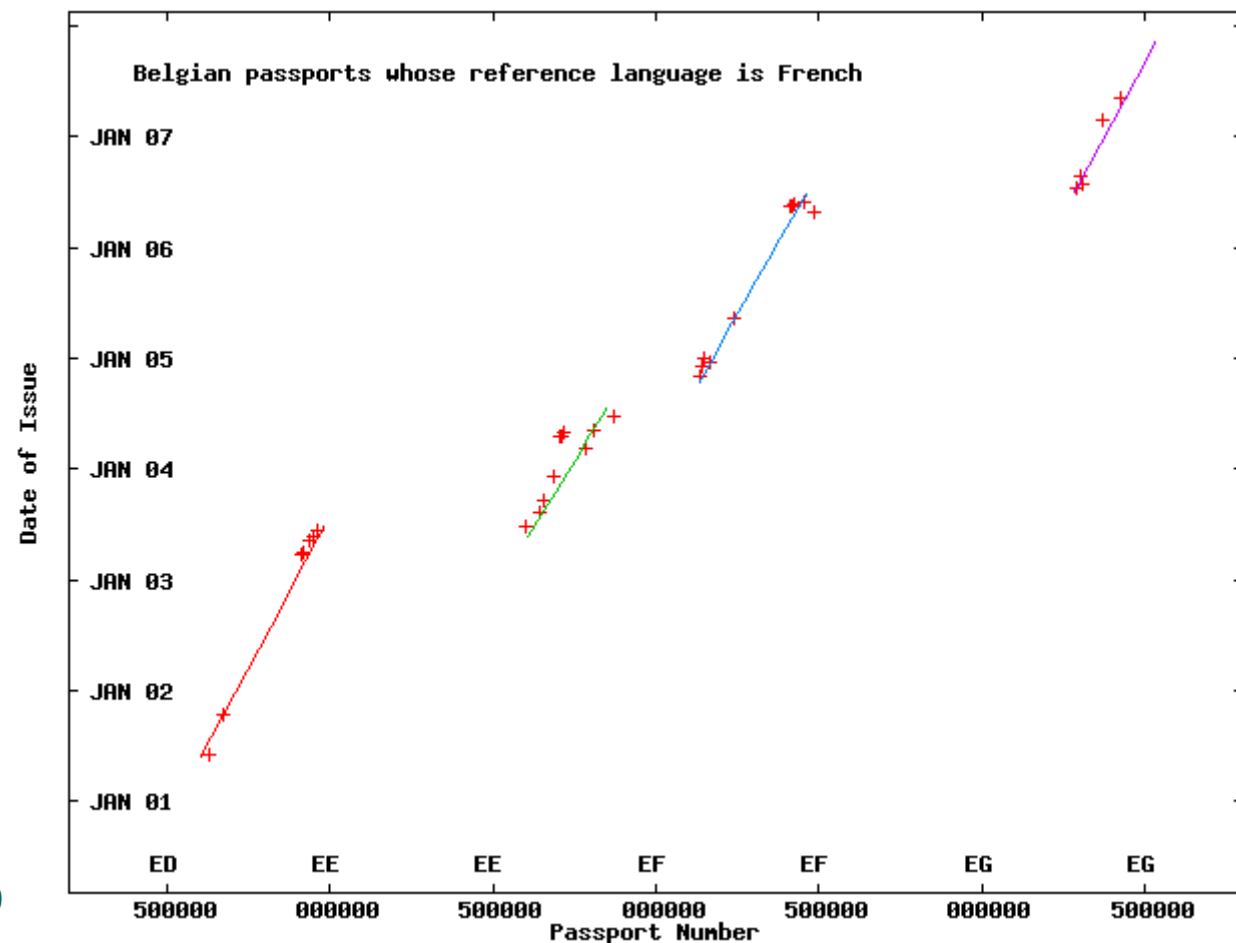
Source: Riscure



Entropy of the key - Belgium

[Avoine, Kalach, and Quisquater] Effective entropy small. ONLINE? attack, trying BAC.

- If the birth date and expiry date are known => the attack takes less than one hour in the worst "common" case (having 24,000 passport numbers to verify at a rate of about 400 checks per minute).



Entropy of the key - Germany

[...] about *40-51 bits* ,
see Christof Paar et al., SHARCS 2007.

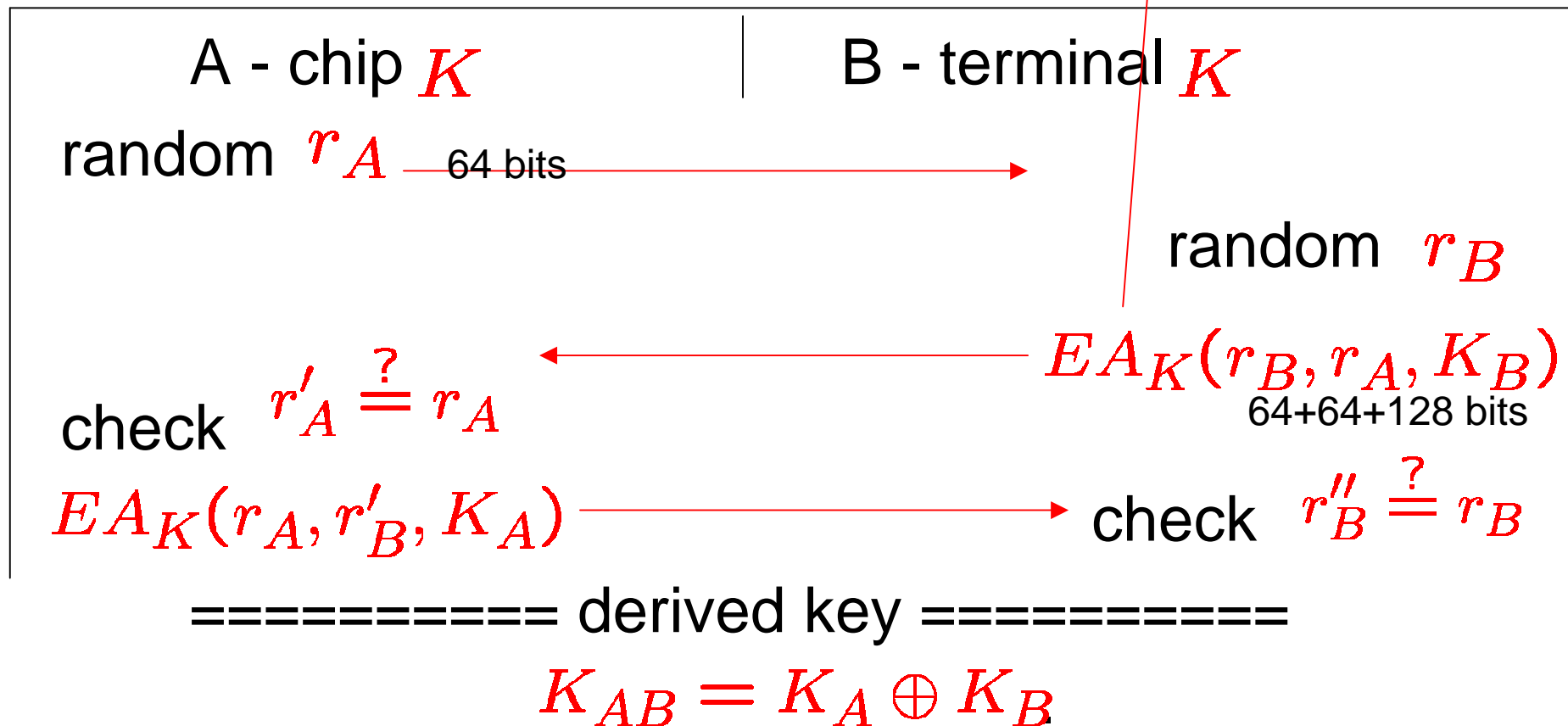
Access Control Almost OK ?

Not at all ! MAJOR FLAW [Wagner et al.]

- ICAO spec.
See it once => access to the passport for eternity...
 - store couples UID???+MRZ
- Example 1: all people that have **ever** been in China in their live, can be traced by the Chinese intelligence.
- Example 2: databases of keys may be compromised/sold and access to all data (including photo biometrics will become public)...

Really? Yes: decrypt this,
keys known

Recall ISO 11770-2 symmetric key establishment





ICAO specs

—

Further Security Aspects



ICAO Proposal – Options, Options

Passive Authentication.

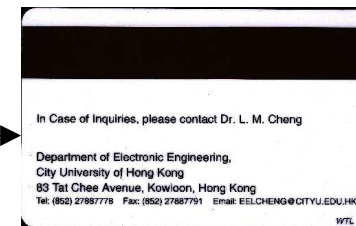
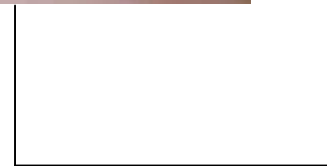
(static RSA/[EC]DSA signature)

The only mandatory mechanism (?!!!!)

Id. Attacks on Identity: Old,

- With no Active Authentication – easy to copy perform impersonation: reuse this static signature.

Skimming Bank Cards



Attacks on ICAO System (1)

Skimming: Much easier, wireless.

Biometric data privacy. ICAO Spec:

- Obligatory: Name, date of birth, passport number, photograph.
- Optional: Nationality, profession, place of birth, address... (the issuing country decides)
 - Also fingerprint/iris

Readable by anyone having MRZ, or breakable...
(seen before)

Attacks on ICAO System (2)

Finding a biometric Twin [Kügler]:

- By stealing real passports: hard and long
- Now easier: can build a machine to detect the person from the distance, one day in big airport...
 - All biometric systems will either fall for it or have a lot of false negatives (can be improved by storing 1000 pictures)
 - Can still be detected by carefully comparing with the picture printed in the passport [but if we can scan it, there is no need for e-passports in the first place...]

Attacks on ICAO System (3)

Skimming: Much easier, wireless.

Prevented by optional PK-based Active Authentication,
but **privacy** problems remain even then:

Challenge Semantics attack [Kügler]:

Transforms a challenge-response system into a “you were there system”, publicly verifiable, based on two signatures:

- The passport signs the challenge
- The terminal signs the challenge with some other data (date, airport, ID of the terminal, etc.).
- The card does not know what it signs, terminal can cheat (unlike in bank cards).

Attacks on ICAO System (4)

Privacy Issues (the same as before)

ICAO-specific issues:

ISO 14443 (contactless and RFID) uses UID value – fixed and different for each passport !!!!!

- tracking,
- hot-listing: building databases
 - CAN BE VERY DANGEROUS:
RFID-enabled bomb !!!
 - Kill a particular individual
 - Kill an American

Attacks on ICAO System (5)

Biometry Issues

Automation/unattended operation:

- In Kuala-Lumpur airport we already have self-service “Auto Gates” ...
- => relaxed human control => more opportunities for fraud/spoofing biometric systems

Optional ICAO Mechanisms

Obligatory:

Access Control, with SK techniques
(+MAC).

Public-key access control would be much
better !

- Active Authentication using PK signatures

PK Authentication Techniques



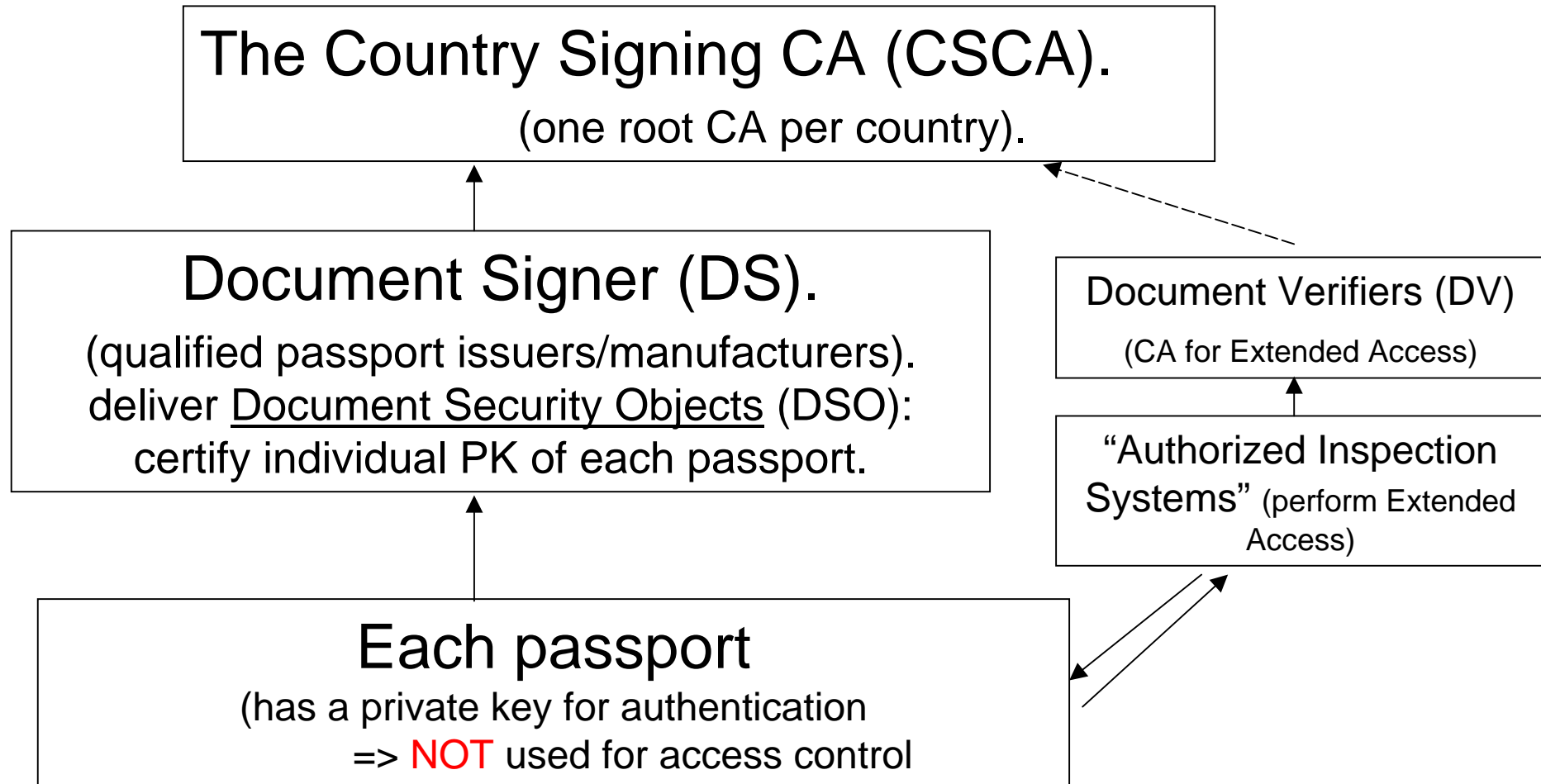


ICAO PKI



ICAO PK-based Authentication

ICAO PKI outline:



Remarks on ICAO PKI

- One root CA per country, no central authority, bilateral key exchange (!),
 - n^2 problem but manageable?
 - there is an attack script on the Internet by creating a new country...
- X.509 certificates are used at high level, not implemented in passport themselves
- CRL are regularly issued by CSCA
 - check all of them (n)



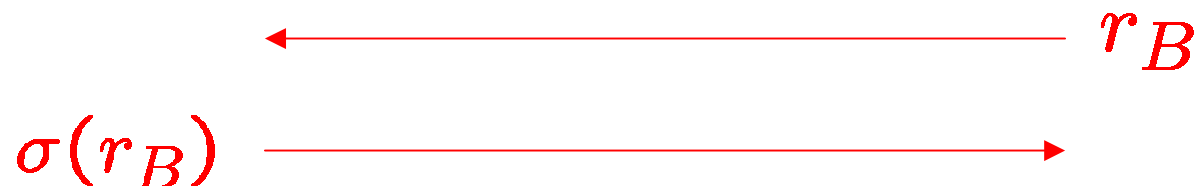
Passive vs. Active Authentication

0. Just basic Passive Authentication, only this is mandatory ...

Just sign the DSO with RSA/DSA/ECDSA, sort of SDA.

1. Active Authentication, optional (equiv DDA)

The card signs a Challenge [RSA,[EC]DSA]



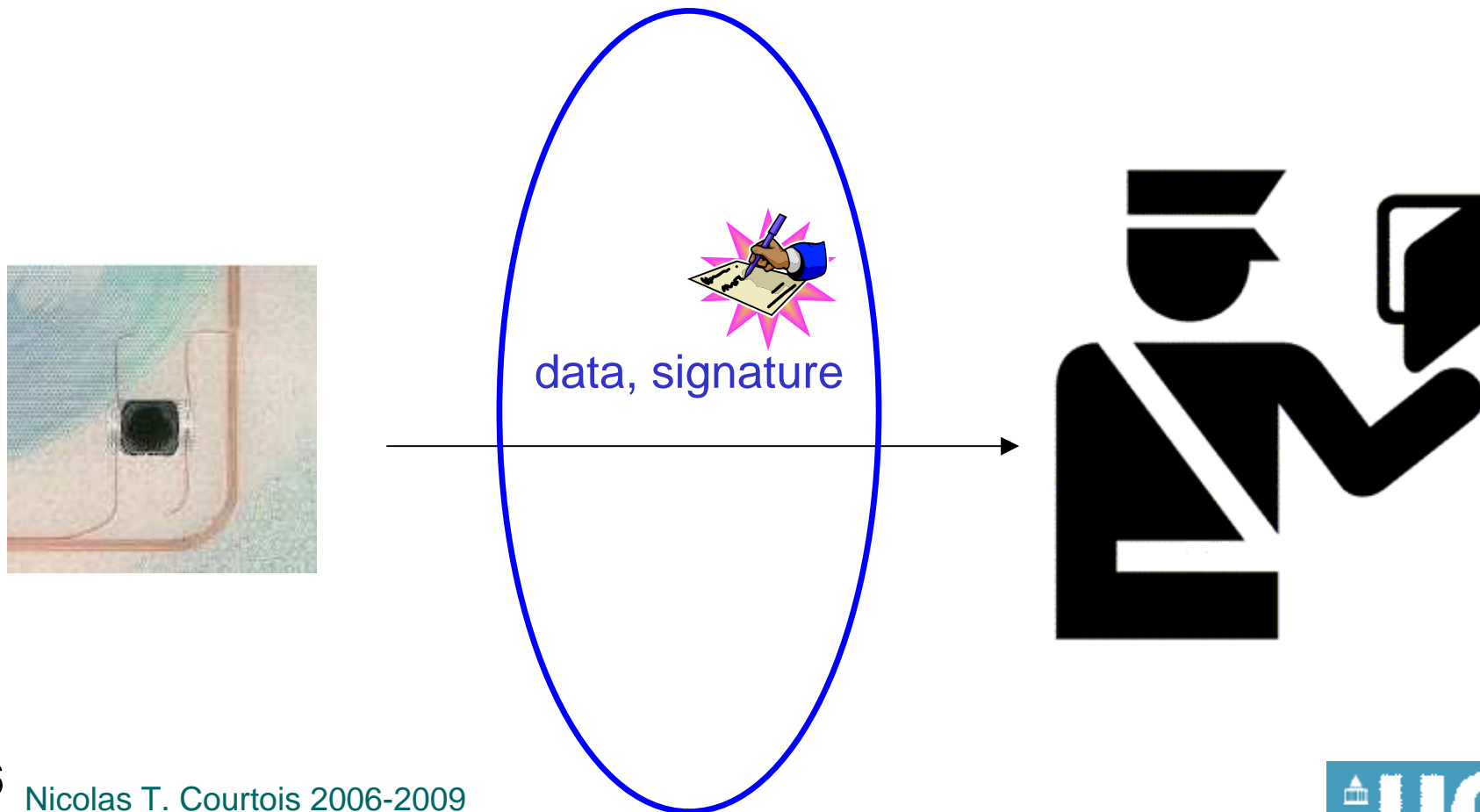


Passive Authentication (PA) (Static Signature)



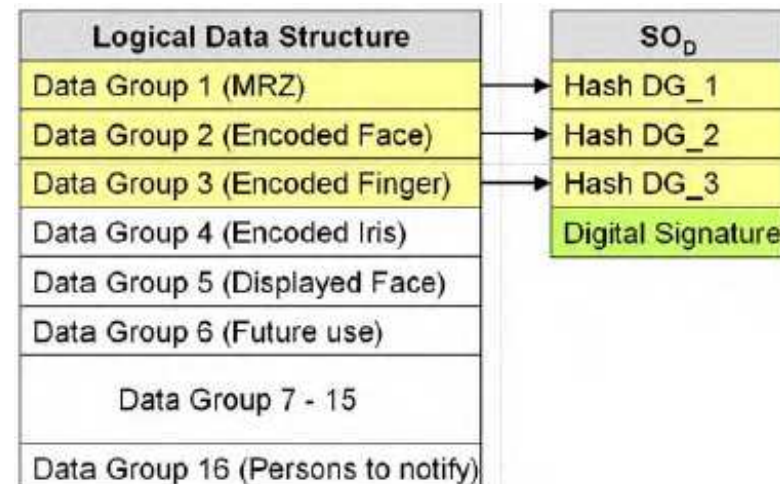
Passive/Static Data Authentication = PA

Signed once for all.



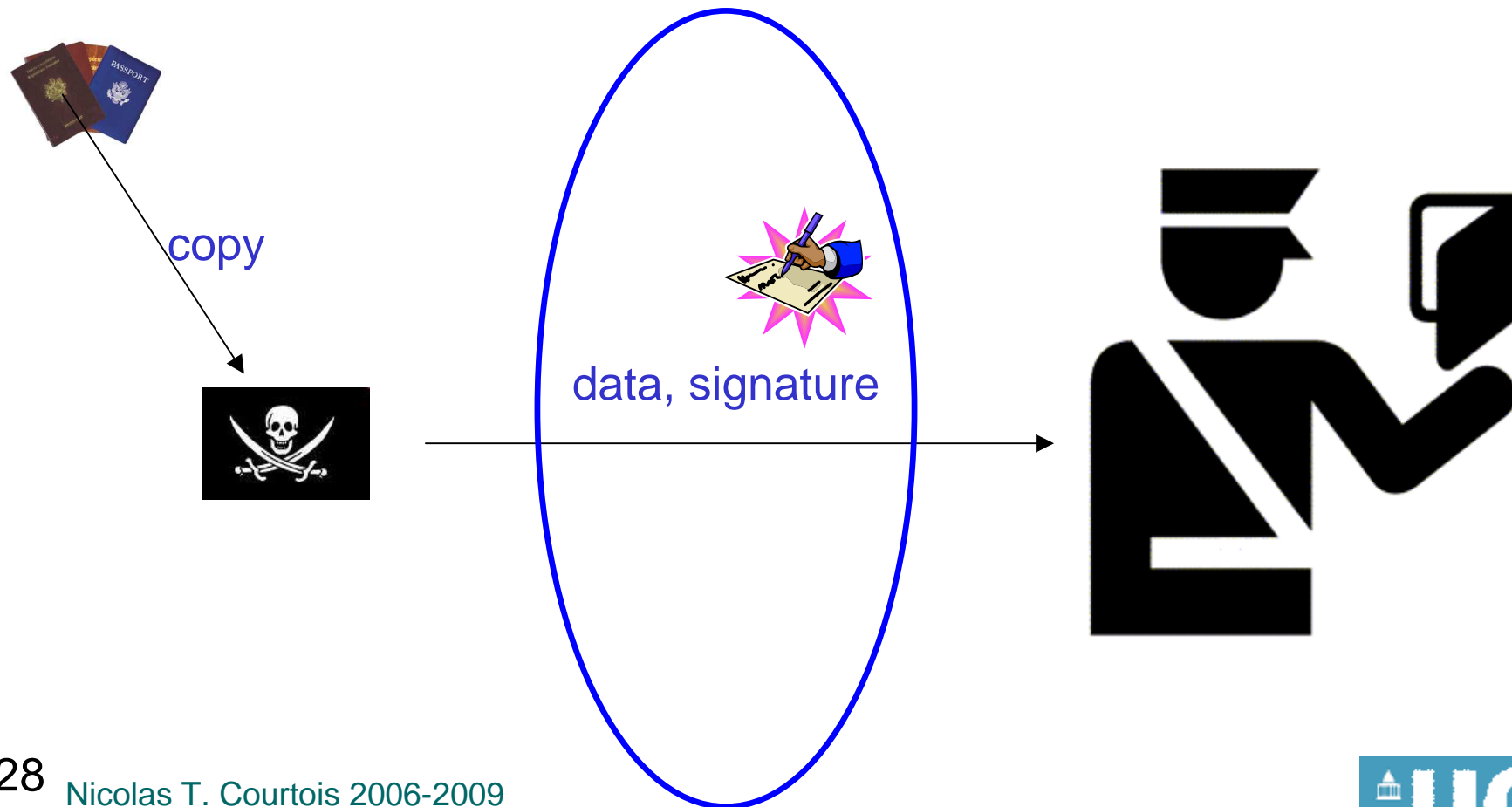
Passive Authentication (PA)

- Always mandatory, present in EF.SOD
(contains the digitally signed list of hashes)
- The list of the hashes (SHA-1/2) of all up to 16 data groups present is digitally signed by the issuer.
 - RSA-2048 minimum
- The DS certificate by CSCS (Country Signing CA – e.g. the ministry of interior) is included
 - ICAO optional, EU mandatory
 - RSA-3072 minimum



PA

Protects against forgery (create a new British citizen)
but still NOT against **copy == passport cloning!**



Active Authentication (AA)

(cf. Dynamic Signatures, DDA)



Active Authentication (Dynamic)

challenge-reply (similar as bank card DDA)

⇒ chip authenticity



Public key is accessible in DG15

⇒ integrity protection: signed by Passive Authentication

Active Authentication (US)

Initially proposed as mandatory in the US passport.

Remains optional [costly, DS by the chip]

For now is used only in some Belgian and Czech passports.

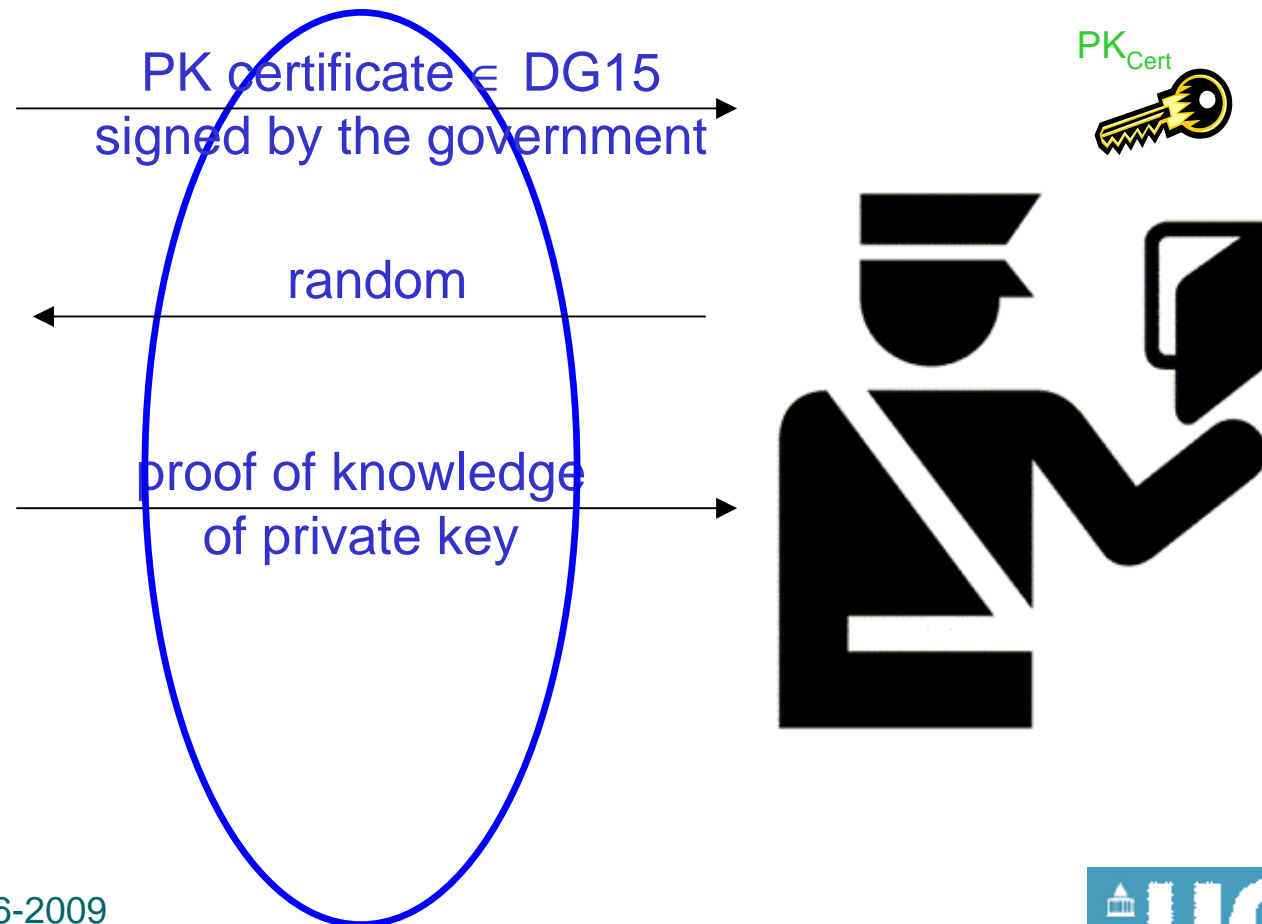


Protects against cloning.

Relay attacks remain possible: eprint.iacr.org/2007/244

AA = Active Authentication

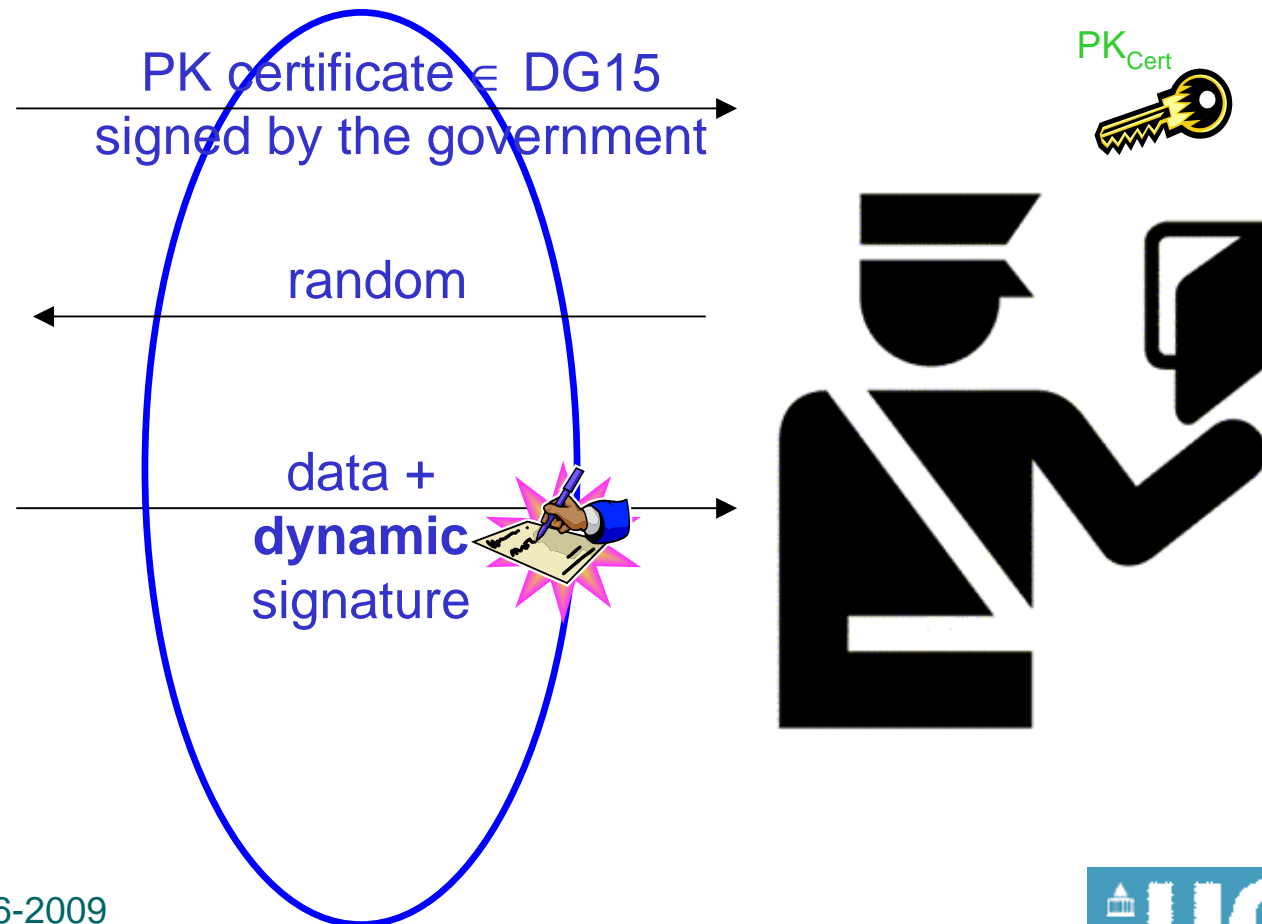
Protects against cloning. More expensive. Optional.



cf. Active / Dynamic Data Authentication



which would be:



So is AA an equivalent of DDA?

Small difference.

In passports the data authenticity is already assured twice:

- by a static signature
- by a MAC during messaging
- [BTW also because cannot be changed]

So only authenticity of the chip is assured by current AA.

(in bank cards, DDA is also a signature of certain data).



Security of ICAO Digital Signature Systems



Signature Schemes and Key Sizes - PA

Hash functions: SHA-1 and all SHA-256

Signature schemes allowed by the specs:

- RSA with PKCS#1 v1.5 padding (min. 3072 bits for CSCA, 2048 bits for DS).
 - Hungary, France, Spain, Portugal, Italy: RSA-4096 + SHA-1
 - Austria, Netherlands: RSA-3072 + SHA-256
- RSA with PSS padding (min 3072 bits for CSCA, 2048 for DS)
 - Czech Republic, Norway, Denmark, Japan and Australia, all+SHA-256
- DSA: not standardized for key lengths > 1024 , not secure enough
- ECDSA (min. 256 bits for CSCA, 224 bits for DS)
 - Switzerland, Germany, Russia: all use SHA-1

Signature Schemes and Keys - AA

AA is not widely deployed as of yet.

In practice only RSA is used

- ISO 9796-2 scheme 1, not proven secure, grey zone
 - Czech Republic, Belgium, Austria,
- DSA and ECDSA also permitted but not widely used for AA

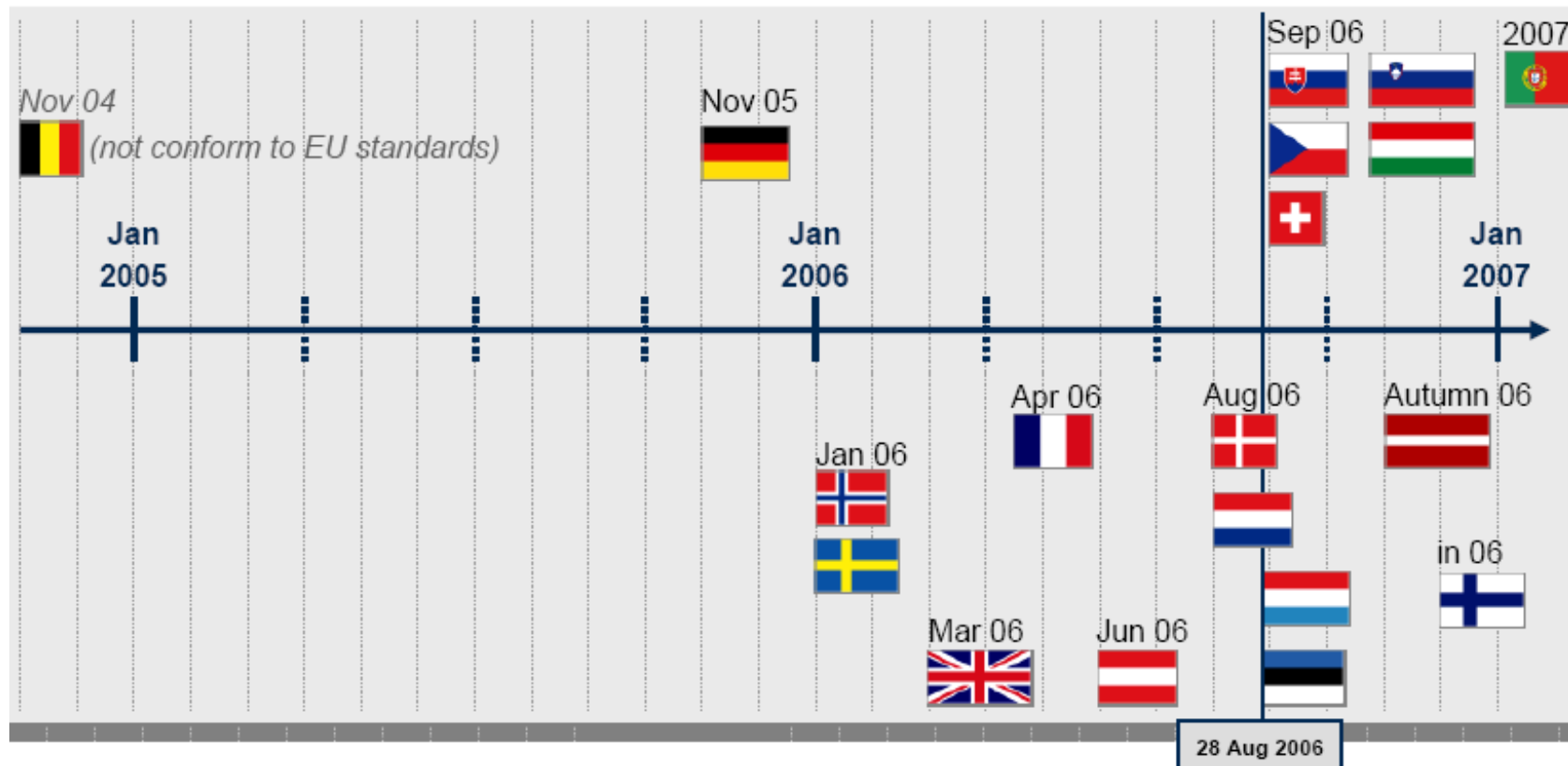


Second Generation Passports [2009]



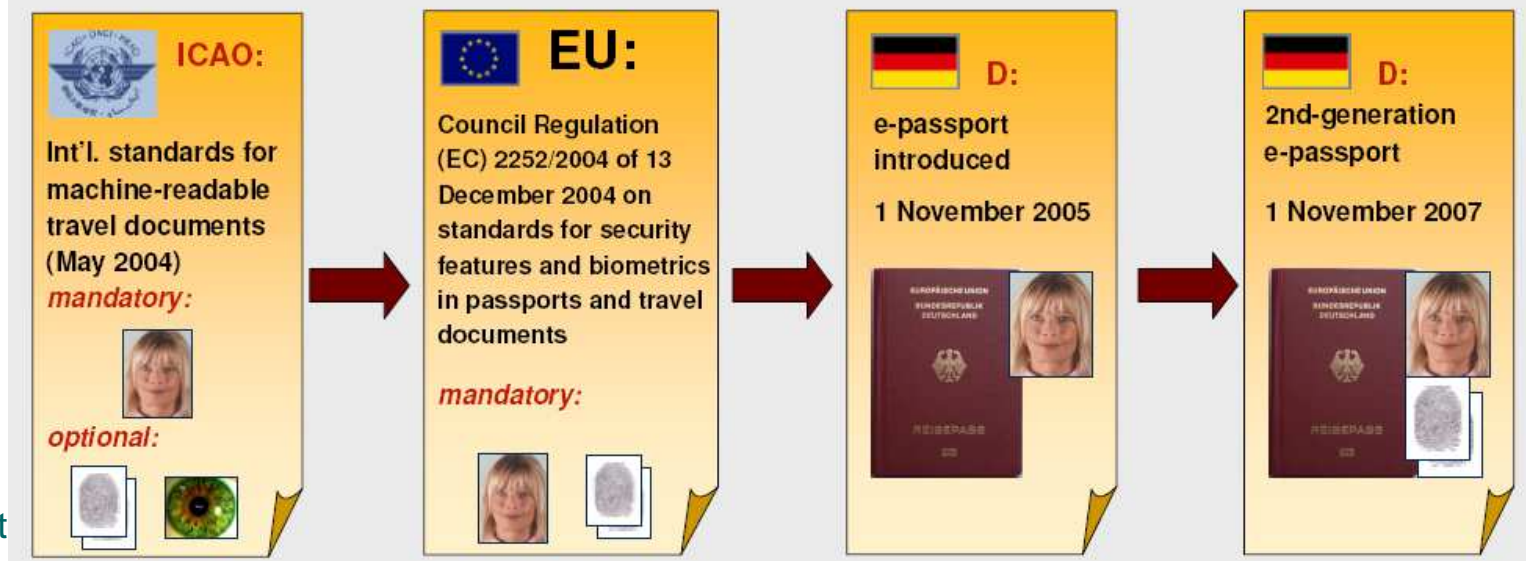
**EU Timeline

European E-Passports



Germany started in 2007

- Dennis Kügler, BSI, though not all his recommendations adopted (yet)
 - BSI Technical Guideline - Extended Access Control:
http://www.bsi.bund.de/.../EACTR*_v*.pdf
http://www.bsi.bund.de/english/publications/techguidelines/tr03110/TR-03110_v200.pdf
 - Security Document World on Extended Access Control:
http://www.securitydocumentworld.com/client_files/eac_white_paper_210706.pdf



Second Generation

EU only, obligatory in June 2009

- based on German proposals...

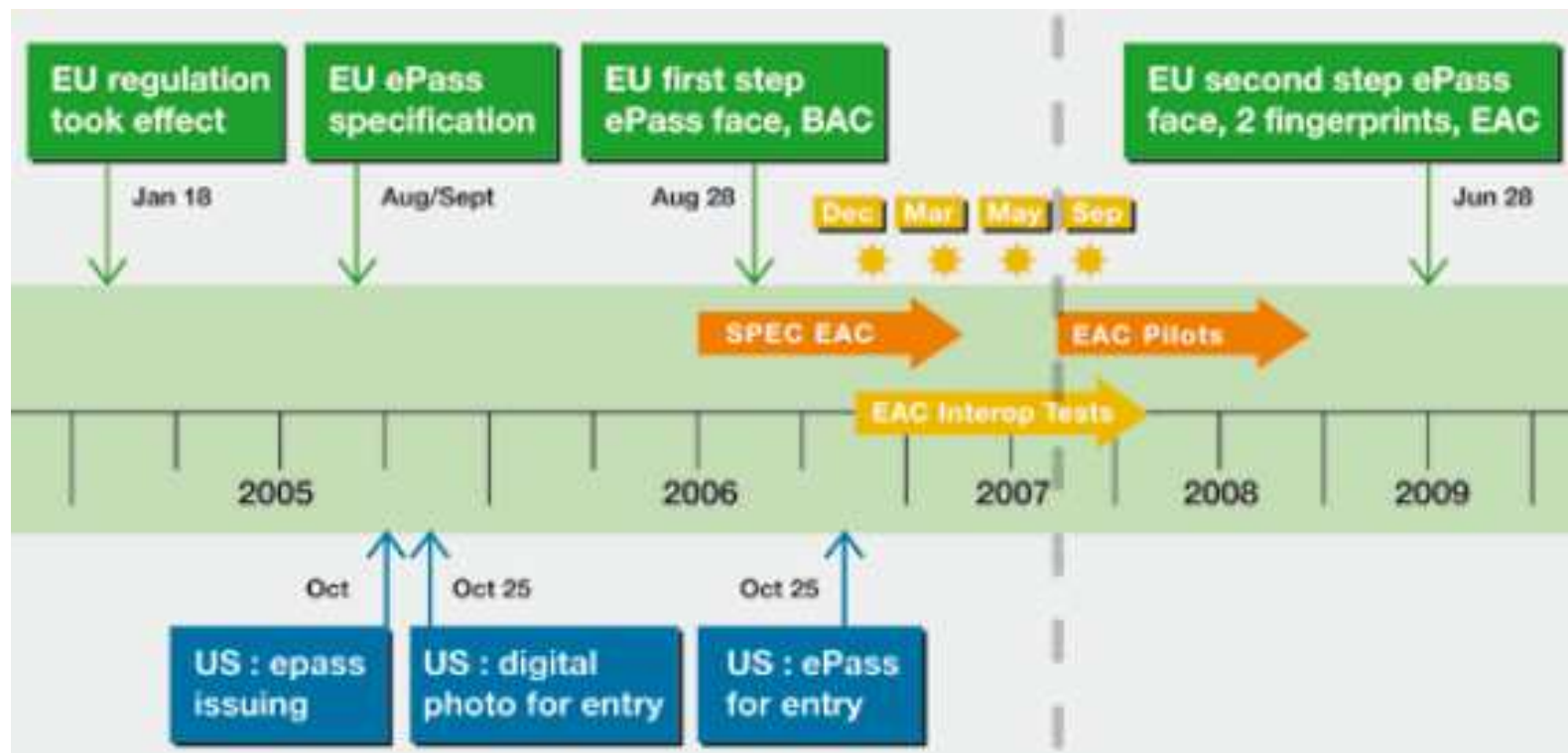


EU vs. US



In the EU ePassports are introduced by the council decision 2252/2004

- Specified by C(2005) 409 and C(2006) 2909
 - Mandatory BAC
 - Optional AA
 - June 2009: mandatory storage of fingerprints + EAC



Second Generation - Summary

- **Extra biometric data:**
 - WG3 fingerprint mandatory
- Terminal → Chip
 - Extended Access Mechanisms mandatory
 - But only for these WG3/4.
- Chip → Terminal
 - Optional (later):
 - BAC revisited (=> PACE)
 - Active Authentication Revisited (Alt. AA)
 - ↓
 - Session Encryption revisited...



Details follow...

**Extra Data

- 2 fingerprints stored as images in WG3
 - obligatory except for small children



More Sensitive DGs

DG	Content	read/write	mandatory / optional	access control
DG1	MRZ	R	m	BAC
DG2	Face	R	m	BAC
DG3	Finger	R	o	BAC+EAC
DG4	Iris	R	o	BAC+EAC
.		R		
DG14	SecurityInfo*	R	o	BAC
DG15	AA public key	R	o	BAC
DG16		R		
SO	Security Object	R	m	BAC

Second Generation - Summary

- Extra biometric data:
 - WG3 fingerprint mandatory
- **Terminal → Chip**
 - **Extended Access Mechanisms mandatory**
 - But only for these WG3/4.
- Chip → Terminal
 - Optional (later):
 - BAC revisited (\Rightarrow PACE)
 - Active Authentication Revisited (Alt. AA)
 - Session Encryption revisited...



Details follow...

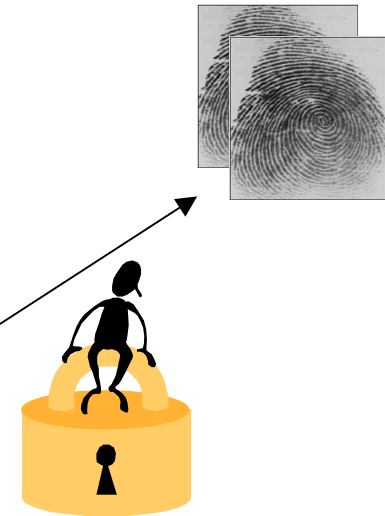
Extra Data of Concern

=> Extended Access Control (EAC),

- mandatory for WG3/WG4,
- high-security, heavy PKI
- access only by
“authorized border authorities”

IS = Inspection System

» The terminal (IS) is also authenticated




EAC Mechanisms



Extra Data + EAC

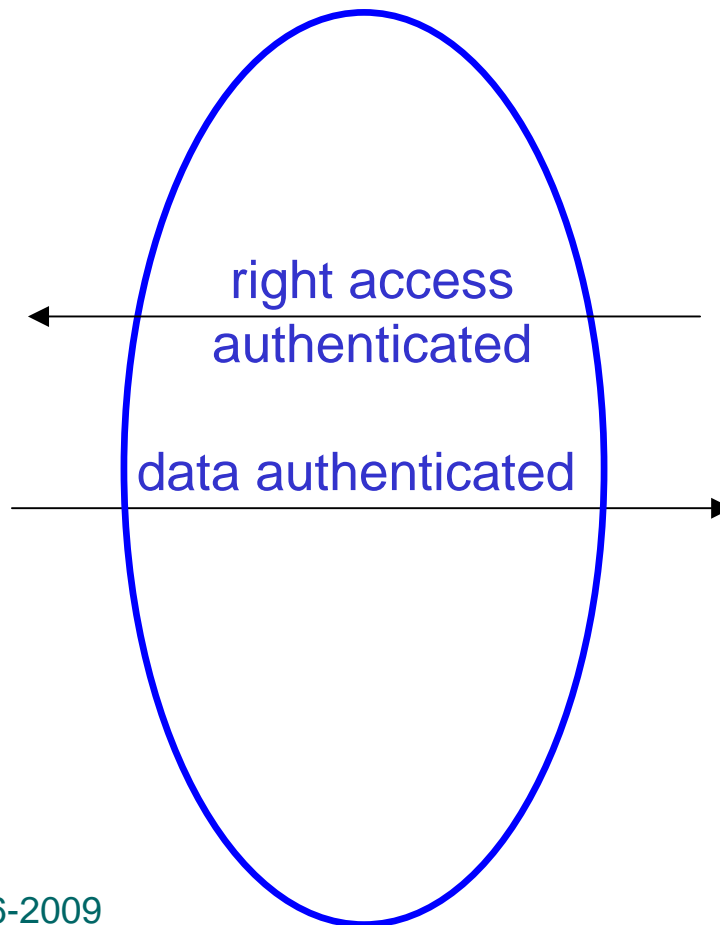
Extended Access Control (EAC),



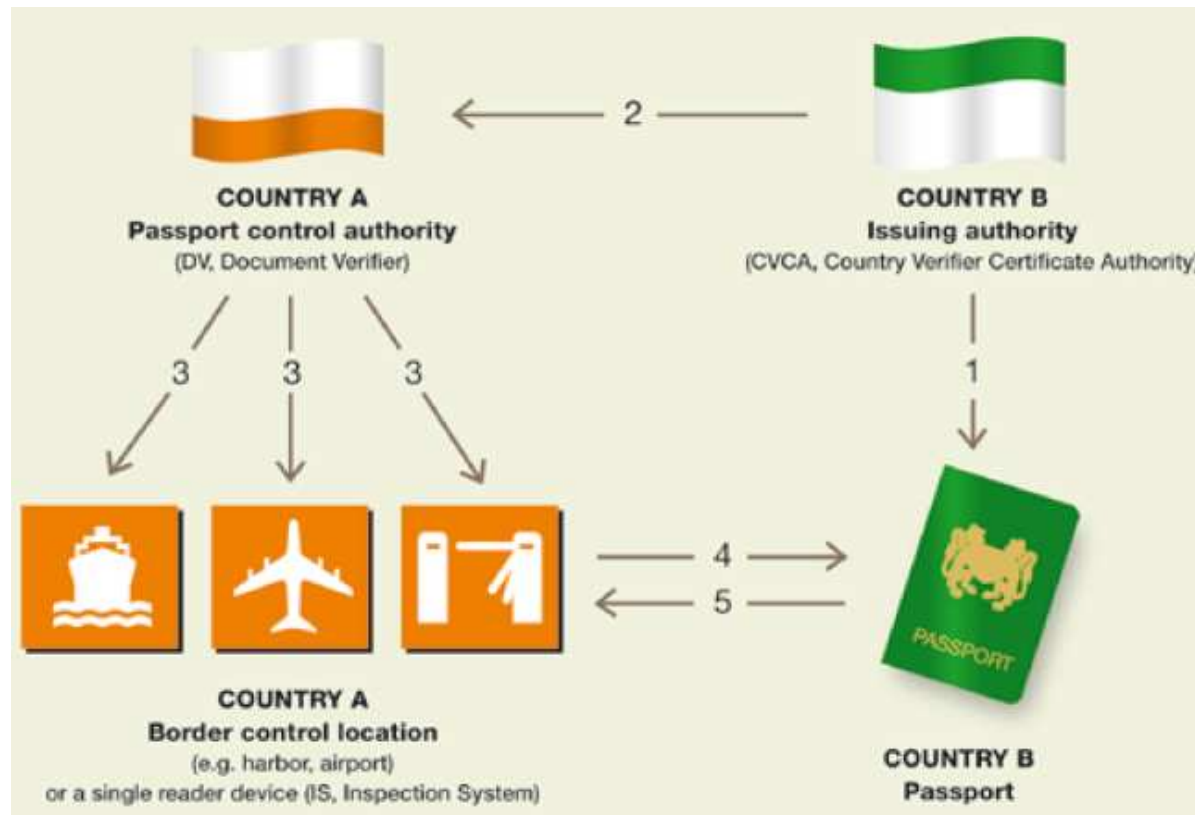
- **Mandatory for DG3,**
 - Systematic in the EU, by law: must use “extended acc.” for biometric data 2008.
- **high-security, heavy PKI**
 - but uses different certificates, ISO7816 card verifiable = CV
- The terminal = **IS** = **Inspection System** is also authenticated
 - must prove it is authorised to read DG3 = 
 - authorization chain:
issuer country -> country2 -> terminal2

Extending Access Control

now mutual



EAC – Authorizing the Terminal



1. CVCA certificate from the issuing country is stored on the passport chip during passport personalization. This certificate will be used to verify the inspection systems certificates (access rights to fingerprint data) in the passport reading step

2. Country B certifies i.e. gives permission to Country A's passport control authority to authorize their access to read the fingerprint data from Country B's passport

3. Country A's border controlling authority certifies i.e. gives permission to its border control locations or individual devices (Inspection Systems) to have an access to read the fingerprint data from Country B's passport

4. Country A's border control reader (Inspection System) shows Country B's passport its authorization to access the fingerprint data on the chip

5. Country B's passport allows reading of fingerprints once the inspection system has proven its authorization from the Country B

Revocation

Great:

With this system country A can distribute to country B **revocable rights**, simply use this PKI and adopt short validity period.

Currently expiry is totally bogus.

Implementation Problem: the passport chip doesn't have a clock, it only records the data of last border control.

- so for people that travel rarely, the access keys will still work and allow to copy their sensitive data...

Forward Secrecy in EAC

Idea:

compromise of the terminal in May
2005, does **not** allow to decipher
previous sessions !!!!

(works only if implementation is correct)

check if works and if really mandatory etc

EAC Crypto

Chip authentication:

- Diffie-Hellman (PKCS#3)
 - 1024 or 1536 bit prime
- Elliptic Curve Diffie-Hellman (ISO 15946, BSI TR-03111)
 - Mostly 224 bit curves, sometimes 256 or 384 bits
- Challenge semantics attacks prevented...

Terminal authentication:

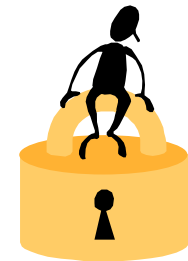
- RSA keys 1024-3072 bits, two signature schemes
 - RSA PKCS#1 v1.5 + SHA-1 or SHA-256 (more popular, grey zone)
 - RSA-PSS, +SHA-1 or SHA-256 (provably secure!)
- ECDSA-160..256 + SHA-1, SHA-224 or SHA-256

Recent Developments and Improvement Proposals



Second Generation - Summary

- Extra biometric data:
 - WG3 fingerprint mandatory
- Terminal → Chip Authentication
 - Extended Access Mechanisms mandatory
 - But only for these WG3/4.
- **Chip → Terminal Authentication**
 - Optional (later):
 - BAC revisited (=> PACE)
 - Active Authentication Revisited (Alt. AA)
 - ↓
 - Session Encryption revisited...



Details follow...



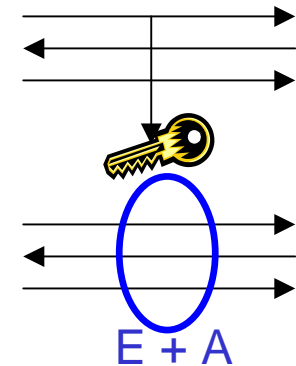
Replace AA

Not yet Mandatory, coexists with PA

1'. Alternative Active Authentication
of the passport.

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ the two are linked!

1'. Session Encryption,
starting from now on.

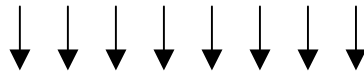




Alternative Active Authentication

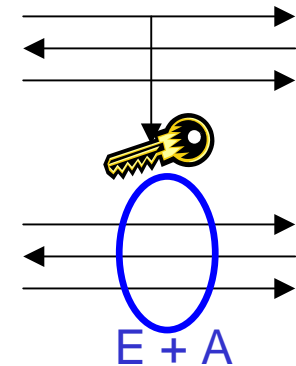
Improves the security of Secure Messaging:

1. Alternative Active Authentication



1'. Session Encryption, starting.

- Keys with much higher entropy than with BAC
- Only an authentic chip can do it,
- **ephemeral**, not eternal
 - (with BAC, once MRZ is known to the attacker, eternal access!)





Alternative Active Authentication

- ElGamal key agreement, based on DH
 - **not-transferable** version of the Active Authentication: Only the reader is convinced (much better privacy, and no abuse such as challenge semantics)
- PK and domain parameters are in DG14
 - Private key never leaves the chip

PACE – added in EAC v2

New password-based access control [2008-9]

- state of the art cryptographic scheme,
- replaces BAC totally
- still not mandatory for DG1,DG2, SOD (would destroy inter-operability).

Conclusion

- Governments obtained what they wanted very quickly
 - US:
 - Initially, inadequate security proposed,
 - Later: “we want security at ANY PRICE“, Wagner et al. paper
 - public comments were received and taken into account.
 - In Europe:
 - many passports in circulation breakable,
 - Hacker scripts circulating on the Internet
 - much higher standards... coming end 2009.
- People obtain what they want much later (more security)
 - this also the interest of Smart card manufacturers
(better chips => higher margins)

Future



Future

- Migrate towards more widespread use of current mechanisms and lower transaction times
 - today: slow to read large files
 - Today few seconds to read a face picture (>20 KB) + digital signatures (10KB)
- Write access - eVisas, eStamps etc.
 - For now all DG are read-only.
- More privacy
 - long list...
 - this requires one worldwide standard
 - so hard to distinguish between passports
 - market consolidation is on the cards...