
EUROPÄISCHE UNION
BUNDESREPUBLIK
DEUTSCHLAND
REISEPASS

DISCALMER

I‘m by no mean an expert in passport and ePassport security. This presentation is just an interpretation of what I understood from the official doumentation. The presentation migh contain mistake or be inaccurate.

1

INTRODUCTION

Why do we need a passport?

> A passport is an official document issued by a government, **certifying** the holder's **identity** and **citizenship** and entitling them to travel under its protection to and from foreign countries.

WHY IDENTIFY?

Uniquely identify you (avoid mismatching)

- Ownership
- Fraud / crime
- Link action / statements (wedding, death, etc)
- Membership (citizen, community, etc)

HOW TO IDENTIFY?

Identity document

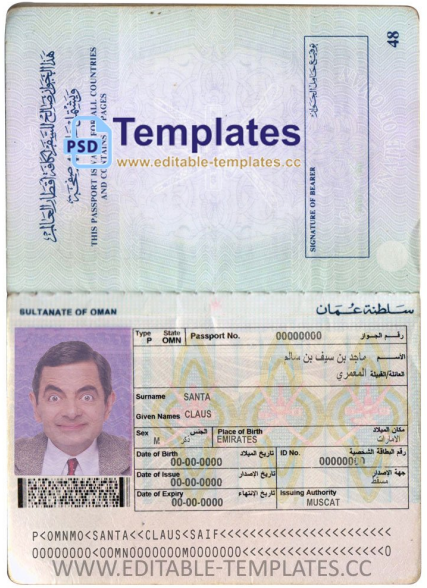
- Request / issuance is controlled
  - Requested by identified parents
  - Birth certificate
- Complex to forge and copy
  - Specific printing technique
  - Signature / Seal
  - Digital certificate

INTERNATIONAL DOCUMENT

- Indicates from which country you are
- Uniquely identify you
  - Request info from origin or other countries
  - Records of past visit

RISKS

- **Data leak**: Unauthorised persons read passport content
- **Copy**: Duplicate your identity
- **Forge**: Create a new identity



IDENTIFY COUNTERFEIT

- Prevent forgery of identity
  - Criminal / Malicious act
- Verify authenticity
  - Uses complex production techniques
  - Provide tool to verify those techniques
- Standardize format and production techniques
  - Simplify verification accross countries
  - Raise forgery complexity to the same level

ADD DIGITAL LAYER

- Raise the forgery complexity
- Automate / Fasten identity verification
- RFID technology
  - Compact (power supply)
  - Cheap and easy to implement
  - Contactless /No need for line of sight
  - Powerful enough for security
  - Large enough memory

2

STANDARDS

Format, technology and communication protocol

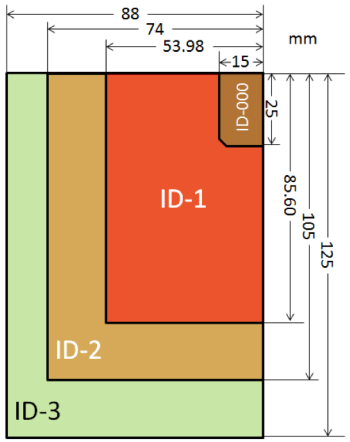
ICAO

International Civil Aviation Organisation (ICAO)

- United Nation specialized agency
- HQ in Montreal, Canada
- Codifies principles and techniques of international air navigation
  - Passport standards recommended to national governments

ISO/IEC 7810

Format	Dimensions	Usage
ID-1	**85.60 x 53.98 mm**	**Banking card & ID**
ID-2	**105 x 74 mm**	**French ID & visas**
ID-3	**125 x 88 mm**	**Passports**
ID-000	**25 x 15 mm**	**SIM cards**



ISO/IEC 14443

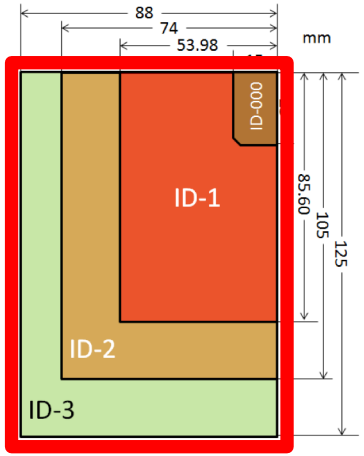
Standard for contactless cards used for identification

- Physical characteristics
- Radio Frequency power and signal interface
- Initialization and anticollision
- Transmition protocol

ISO/IEC 14443

Physical characteristics

- ISO/IEC 7810 compliant
- ISO/IEC 15457-1 compliant
- „an object of any dimensions“

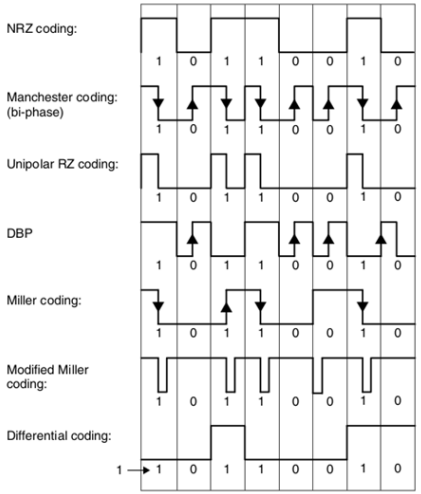


ISO/IEC 14443

Radio Frequency power and signal interface

- 13.56 MHz
- Type A
- Type B

	Encoding	Modulation
Type A	**Miller (delay)**	**Amplitude (100%)**
Type B	**Manchester**	**Amplitude (10%)**



ISO/IEC 14443

Initialization and anticollision

- Chip has a Unique Identifier (UID)
- Type A: Bit anticollision
- Type B: Based on slot marker

ISO/IEC 14443

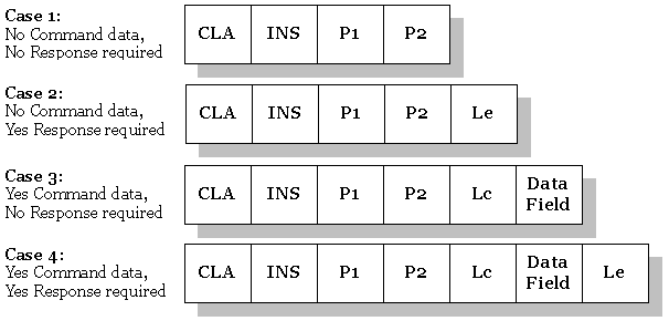
Transmition protocol

- Advertisement of protocol parameters
  - Type A: Answer to Select (ATS)
  - Type B: Answer to Request Type B (ATQB)
- Application Protool Data Units (APDU)ISO/IEC 7816-4s
  - ISO/IEC 7816-4

Application Protocol Data Unit (APDU)

Command

4 byte header + 0..255 bytes data

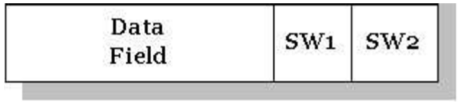


- **CLA**: Instruction class (type of command)
- **INS**: Instruction code (specific command)
- **P1-P2**: Instruction parameters for the command
- **Lc**: Length of data (byte)
- **Data field**: Command data (length = **Lc**)
- **Le**: Max length (byte) expected for response

Application Protocol Data Unit (APDU)

Response

0..65536 bytes data + 2 status bytes



- **Data field**: Response data (length <= **Le**)
- **SW1**-**SW2**: Command processing status

ISO/IEC 7501-1 (DOC 9303)

- Machine Readable Zone (Part 3)
- Logical Data Structure (Part 10)
- Security measures (Part 11)

ISO/IEC 7501-1 (DOC 9303) - MRZ

Machine Readable Zone (MRZ)

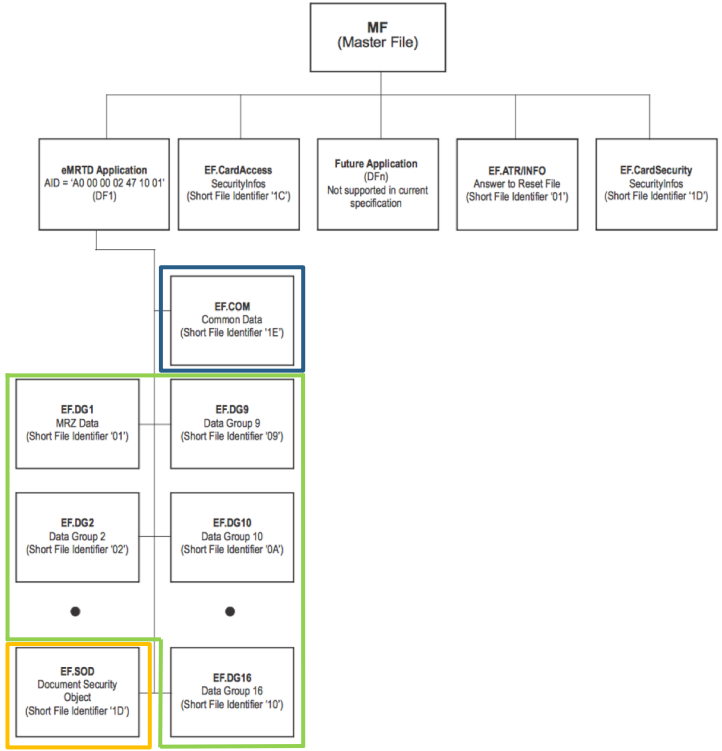
Document type
Issuing country
Last name
Given name

```
P < D << MUSTERMANN  <<  ERIKA  <<<<<<<<<<<<<<<<<<<<<<
C01X00T47 8 D << 640812 5 F 270228 3 <<<<<<<<<<<<<< 4
```

Document number
Check digit
Nationality
Date of birth
Check digit
Gender
Expiration data
Check digit
Check digit

ISO/IEC 7501-1 (DOC 9303) - LDS

Logical Data Structure (LDS)



- **MF**: Master File
- **DF**: Dedicated File
- **EF**: Elementary File
- **DG**: Data Group
- **eMRTD**: electronic Machine Readable Travel Document

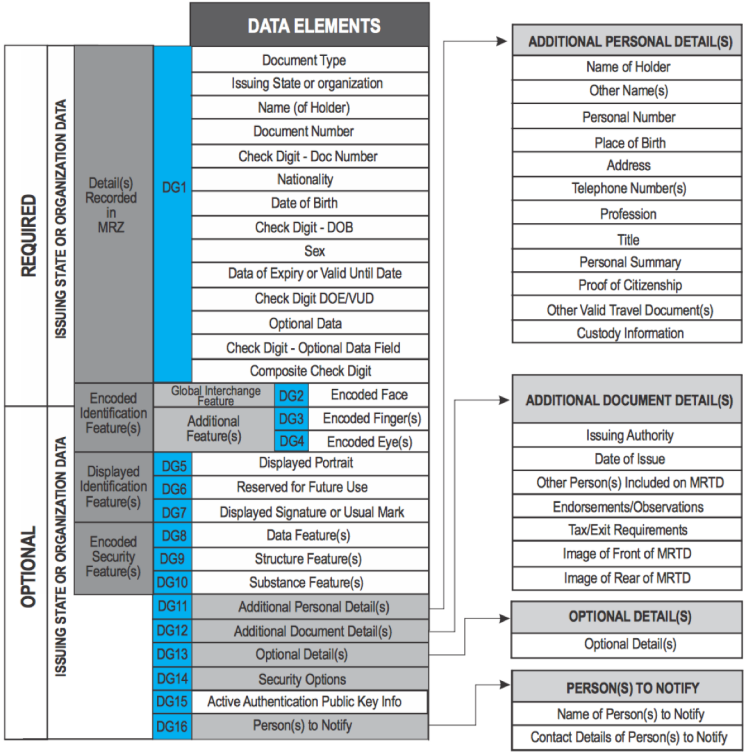
Logical Data Structure (LDS) – Common Data

Common Data (EF.COM)
LDS Version number with format aabb, where aa defines the version of the LDS and bb defines the update level.
Unicode Version number with format aabbcc, where aa defines the major version, bb defines the minor version and cc defines the release level.
Tag list. **List of all Data Groups** present.

ISO/IEC 7501-1 (DOC 9303) - LDS

Logical Data Structure (LDS)

Data Group



Logical Data Structure (LDS) – Document Security Object

Document Security Object ($EF.SO_D$)
This object is digitally signed by the issuing State and contains **hash** values of the LDS contents.

ISO/IEC 7501-1 (DOC 9303) – SECURITY

Security Measures

- Basic Authentication Control
- Passive Authentication
- Active Authentication
- Password Authenticated Connection Establishment
- Extended Access Control

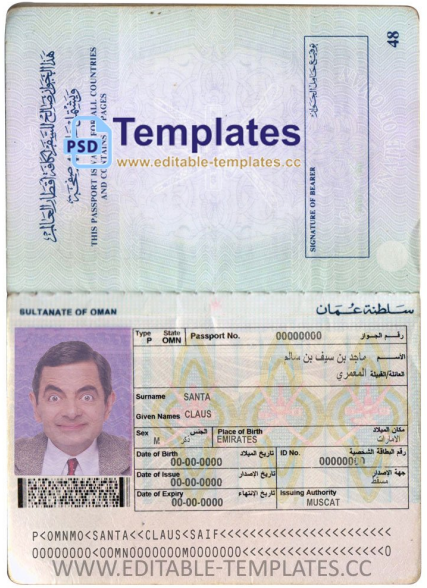
3

SECURITY MEASURES

As defined in ISO/IEC 7501-1 (DOC 9303)

RISKS

- **Data leak**: Unauthorised persons read passport content
- **Copy**: Duplicate your identity
- **Forge**: Create a new identity



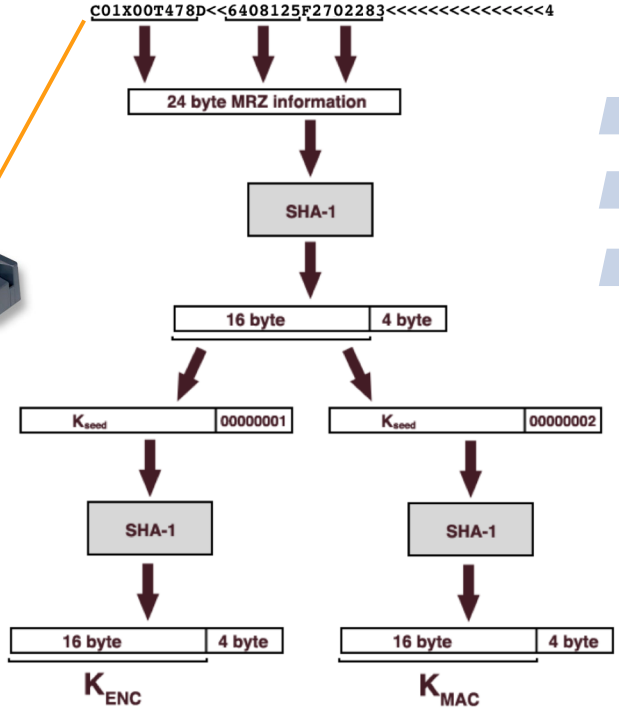
BASIC AUTHENTICATION CONTROL (BAC)

Basic Authentication Control is meant to calculate keys based on the MRZ:

- Session encryption key
- Session MAC key
- Session sequence counter

BASIC AUTHENTICATION CONTROL (BAC)

Basic Access Keys

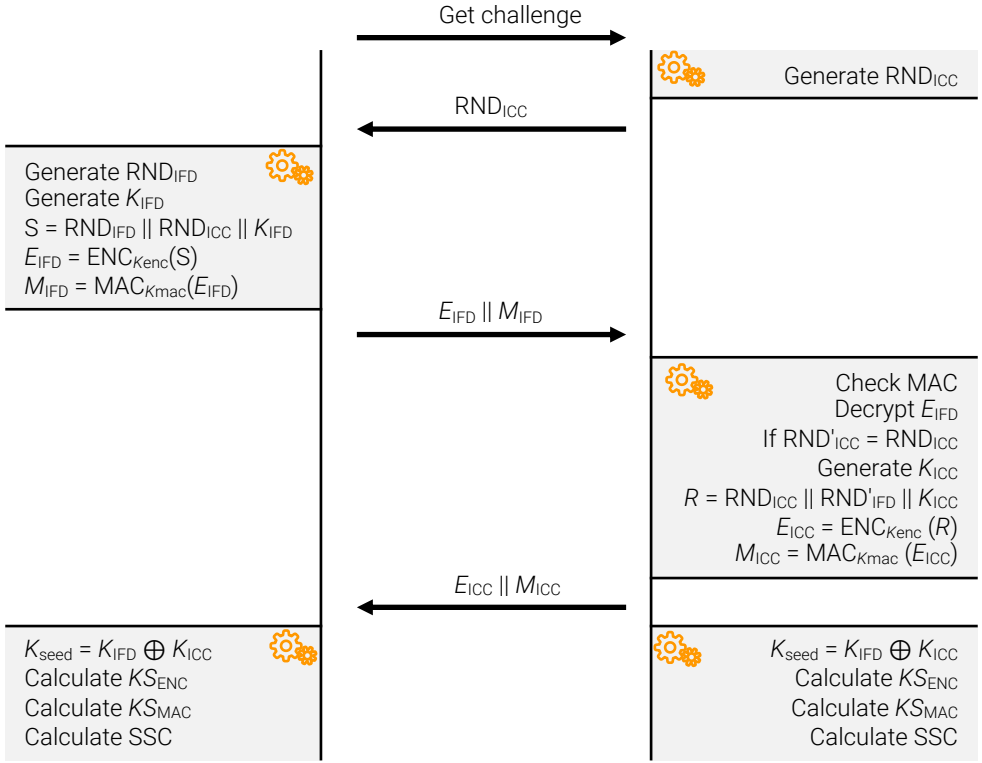


- Pass-Nr
- DoB + check digit
- Exp data + check digit

BASIC AUTHENTICATION CONTROL (BAC)

IFD = InterFace Device
Passport reader

ICC = Integrated Circuit Card
Passport



RND = Random Number (8-bytes)
K = Key (16 bytes)
M = MAC (8 bytes)
ENC = 3DES encryption
MAC = MAC Algorithm 3
KS = Final keys for session
SSC = Send Sequence Counter

BASIC AUTHENTICATION CONTROL (BAC)

Compute session keys from key seed

KS_{ENC}

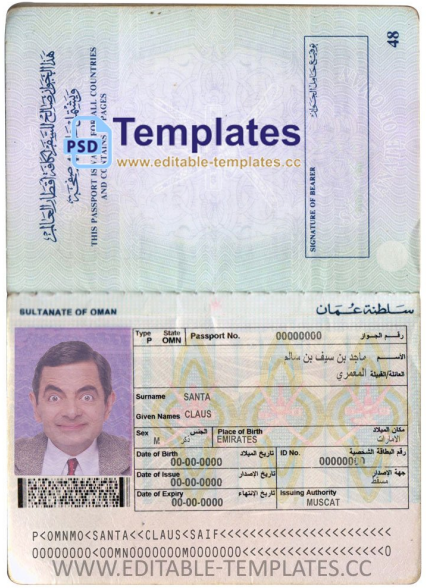
- $D = K_{seed} \,||\, 00000001$
- $H = HASH_{SHA\text{-}1}(D)$
- $K_{a'} = H[0:8]$ and $K_{b'} = H[8:16]$
- Adjust parity for $K_{a'}$ and $K_{b'}$
- K_a and K_b are used as first and second key for 3DES

KS_{MAC}

- $D = K_{seed} \,||\, 00000002$
- $H = HASH_{SHA\text{-}1}(D)$
- $K_{a'} = H[0:8]$ and $K_{b'} = H[8:16]$
- Adjust parity for $K_{a'}$ and $K_{b'}$
- K_a and K_b are used as first and second key for MAC

RISKS

- ~~**Data leak**: Unauthorised persons read passport content~~
- **Copy**: Duplicate your identity
- **Forge**: Create a new identity



PASSIVE AUTHENTICATION (PA)

Verify integrity of the passport

- $EF.SO_D$ contains hash of the LDS
- $EF.SO_D$ is digitally signed by issuing country
- $EF.SO_D$ contains the Document Signer Certificate (C_{DS}) used to sign $EF.SO_D$

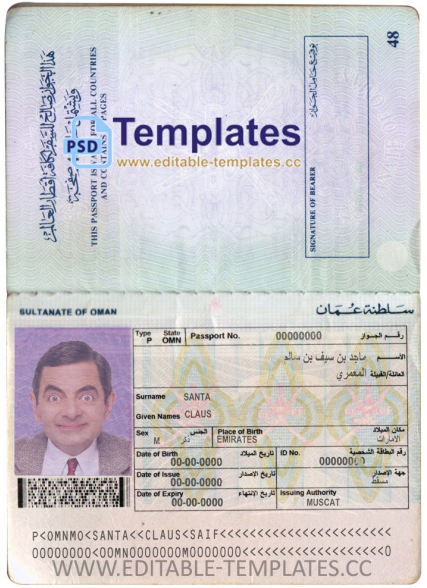
PASSIVE AUTHENTICATION (PA)

Inspection process

- Read the SO_D (C_{DS}, DGs hashes, and signature)
- Build and validate path from Trust Anchor to the *Document Signer Certificate* (C_{DS})
- Use the verified *Document Signer Public Key* (KPu_{DS}) to verify the SO_D signature
- When reading a DG, verify its hash

RISKS

- ~~**Data leak**: Unauthorised persons read passport content~~
- **Copy**: Duplicate your identity
- ~~**Forge**: Create a new identity~~



ACTIVE AUTHENTICATION (AA)

Authenticate the passport (IC)

- The IC has its own AA key pair (KPr_{AA} and KPu_{AA})
- KPu_{AA} is located in the DG15
- KPr_{AA} is located in the IC‘s secure memory

ACTIVE AUTHENTICATION (AA)

IFD = InterFace Device
Passport reader

Generate M_2

M_2 →

(Based on ISO/IEC 9796-2)
Create T
Generate M_1 of L_{M1}bits
$M = M_1 \parallel M_2'$
$H = \text{hash}(M)$
$F = \texttt{0x6A} \parallel M_1 \parallel H \parallel T$
$S = \text{ENC}_{\text{PrK}}(F)$

← S

Decrypt S' with PuK_{DG15}
$D = \text{hash}(M_1' \parallel M_2)$
Check if $D = H'$

ICC = Integrated Circuit Card
Passport

M_1 = Random Number (L_{M1} bits)
M_2 = Random Number (8-bytes)
L_{M1} is adjusted to avoid padding
T = Trailer incl. hash algo
ENC = RSA (or ECDSA)

ADDITIONAL

Improve initial security mechanisms and introduce new features

PASSWORD AUTHENTICATED CONNECTION ESTABLISHEMENT (PACE)

Improve BAC by computing strong session key

despite the low entropy shared secret

PASSWORD AUTHENTICATED CONNECTION ESTABLISHEMENT (PACE)

IFD = InterFace Device
Passport reader

ICC = Integrated Circuit Card
Passport

IFD		ICC
π = MRZ or CAN $K\pi$ = SHA-1(π || 3)		Generate RND_{ICC} $z = ENC_{K\pi}(RND_{ICC})$
	$z + D_c$	
$RND'_{ICC} = DEC_{K\pi}(z)$		
	data for **mapping**	
Compute D Generate SK_{IFD} and PK_{IFD}		Compute D Generate SK_{ICC} and PK_{ICC}
	PK_{IFD}, PK_{ICC}	
Check $PK_{IFD} \neq PK_{ICC}$ $K = KA(SK_{IFD}, PK_{ICC}, D)$ $KS_{MAC} = KDF_{MAC}(K)$ $KS_{ENC} = KDF_{ENC}(K)$ $T_{IFD} = MAC(KS_{MAC}, PK_{ICC})$		Check $PK_{IFD} \neq PK_{ICC}$ $K = KA(SK_{ICC}, PK_{IFD}, D)$ $KS_{MAC} = KDF_{MAC}(K)$ $KS_{ENC} = KDF_{ENC}(K)$ $T_{ICC} = MAC(KS_{MAC}, PK_{IFD})$
	T_{IFD}, T_{ICC}	

CAN = Card Access Number
$K\pi$ = Derived key from π
RND = Random Number
mapping = map a random number to parameters used for asymmetric cryptography
D = Ephemeral domain parameters
SK = Diffie-Hellman secret key
PK = Diffie-Hellman public key
K = Shared secret
KA = Diffie-Hellman key agreement
KS = Session key
KDF = Key derivation function
T = Authentication token

EXTENDED ACCESS CONTROL (EAC)

- Biometric in passport
  - Picture (mandatory – accessible with BAC/PACE)
  - Fingerprint
  - Iris
- Document issuer decide who can access data
  - National
  - Bilateral use
- Document issuer decide how to protect
  - Encryption
  - Access restriction

EXTENDED ACCESS CONTROL (EAC)

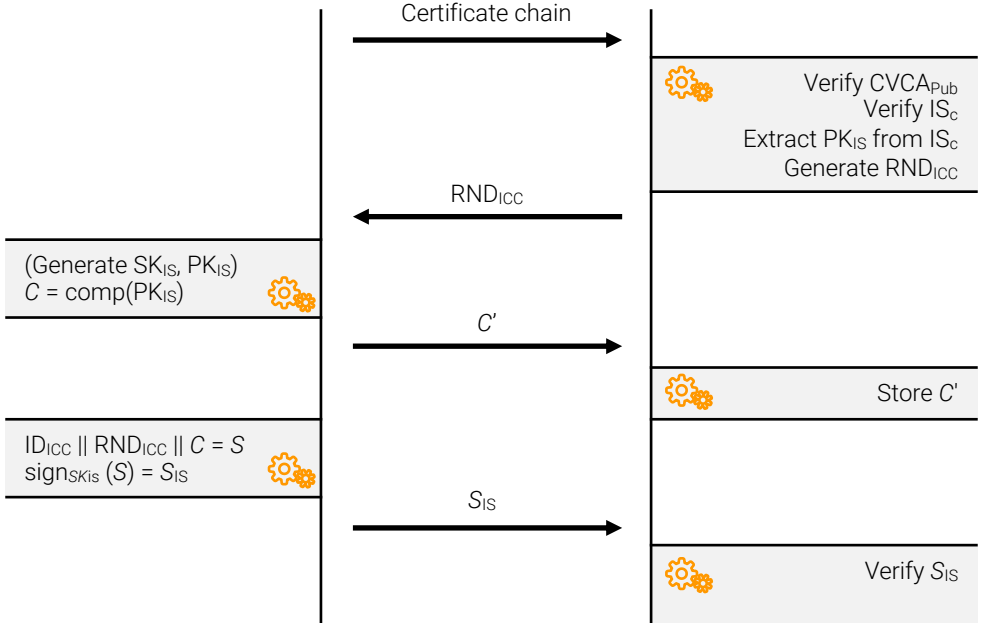
- Uses different keys then BAC/PACE
  - Document Extended Access Keys
  - Symmetric keys or asymmetric key pair
- Document issuer decide how to implement
- BSI (Germany) published EU specifications
  - Chip Authentication
  - Terminal Authentication

TERMINAL AUTHENTICATION (BSI TR-03110)

- TA (when implemented) should be done before CA
- Country Verifying CA
  - Public key stored in passport
  - Deliver certificate for inspection systems (passport readers)

TERMINAL AUTHENTICATION (BSI TR-03110)

IS = Inspection system
Passport reader



ICC = Integrated Circuit Card
Passport

Cert. chain = $CVCA_{Pub}$ + IS_c

IS_c = IS certificate

RND = Random number

SK_{IS} = DH secret key (from PACE)

PK_{IS} = DH public key (from PACE)

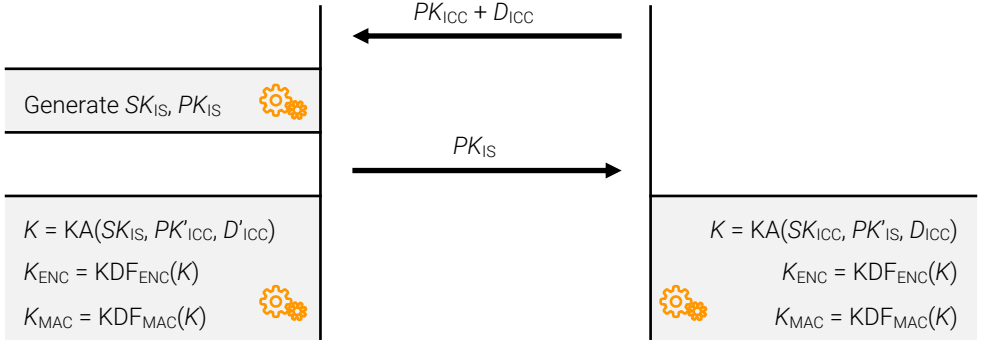
C = Compressed ephemeral key

CHIP AUTHENTICATION (BSI TR-03110)

- Creating strong K_{ENC} and K_{MAC} for communication
- K_{ENC} and K_{MAC} are compute via DH key agreement protocol
- Passport has static DH public and private keys
- Must be combine with Passive Authentication

CHIP AUTHENTICATION (BSI TR-03110)

IS = Inspection system
Passport reader



ICC = Integrated Circuit Card
Passport

D = Domain parameter
PK = DH public key
SK = DH secret key
KA= DH key agreement protocol
KDF = Key derivation function
C = Compressed ephemeral key

4

VULNERABILITIES

How secure is your passport?

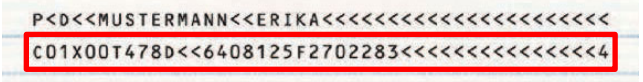
OBJECTIVES

- Trace the holder (anonymously)
- Get some information about the holder
- ~~Read the entire content of the passport~~
- ~~Forge valid passport~~

KNOWN VULNERABILITIES

- MRZ low entropy
- Timing attack
- Fingerprint methods
- NULL random number
- Early Active Authentication

MRZ LOW ENTROPY



- Passport number
- Date of birth + ~~check digit~~
- Expiration date + ~~check digit~~

	Entropy
Pass n°	• **Alphanumeric** • **Has pattern** • **Sometime sequential**
DoB	• **Can be approximated** • **~100 x 365 max**
Exp. date	• **Usually 5 to 10 years**

MRZ LOW ENTROPY

Online brute-force attacks

- Stand next to victim
- Execute BAC and iterate through defined MRZ range
- 43,5 MRZ / s (tested on BE passport)
- Countermeasures
  - Force connection to reset after one fail
  - Increase time to proceed BAC
  - RFID shield
  - Use PACE

MRZ LOW ENTROPY

Offline brute-force attacks

- Caputre one valid BAC transaction
- Iterate through defined MRZ range and generate K_{MAC}
- Verify if MAC(E_{IFD}) = M_{IFD}
- Much faster (+`100x` online brute force)
- Countermeasures
  - Increase complexity for eavesdropping
  - Use PACE

MRZ LOW ENTROPY

Lookup table

- 00‘s padding in old Italian passports
  - `GET CHALLENGE` with `Le` set to `0x01`
  - Response will return one byte padded with `0x00`‘s
- MITM attack
- Brute force GET CHALLENGE until you get only 00‘s
- Pre-build a lookup table to find K_{ENC}

```
PA DD IN G. PA DD IN G.
00 00 00 00 00 00 00 00
```

MRZ LOW ENTROPY

IFD = InterFace Device
Passport reader

ICC = Integrated Circuit Card
Passport

GET CHALLENGE

(1)

GET CHALLENGE
(LE = 0x01)

Generate RND_{ICC}

RND_{ICC}

00 00 00 00 00 00 00 00

If $RND_{ICC}[0] \neq 0x00$:
Go to (1)

Calculate *S*
$E_{IFD} = ENC_{Kenc}(S)$
$M_{IFD} = MAC_{Kmac}(E_{IFD})$

$E_{IFD} \parallel M_{IFD}$

$E_{IFD} \parallel M_{IFD}$

Calculate *R*
$E_{ICC} = ENC_{Kenc}(R)$
$M_{ICC} = MAC_{Kmac}(E_{ICC})$

$E_{ICC} \parallel M_{ICC}$

$E_{ICC} \parallel M_{ICC}$

Lookup for KENC where
$ENC_{KENC}(\{0x00\}^8) = E_{ICC}[0:8]$

R = $RND_{ICC} \parallel RND'_{IFD} \parallel K_{ICC}$

ENC = 3DES – CBC – Null IV

EARLY ACTIVE AUTHENTICATION

- Some passports accept AA before BAC and PA
- You can sign anything
  - Proof that you met the victim
  - Approximate modulo for traceability
    - Send many random values to sign
    - Keep the higest signed value

TIMING ATTACK

- Passports first verify the M_{IFD} then RND_{ICC} in BAC
- If M_{IFD} is not valid, the passport will throw an error
- The time for decryption + RND_{ICC} verification is measurable

  ↳ Possible to track user

TIMING ATTACK

Attack

- Caputre one valid BAC transaction
- Initiate the BAC and re-sent the E_{IFD} || M_{IFD}
- Calculate the time (T_1) for the entire process
- Re-initiate the BAC but send a random E_{IFD} || M_{IFD}
- Calculate the time (T_2) for the entire process
- If T_2 is significantly faster than T_1 , it means the passport is the same

FINGERPRINTING METHODS

- Error Message (malformed APDU)
- Answer to Reset (ATR)
- Unique IDentifier (UID)
- Response time

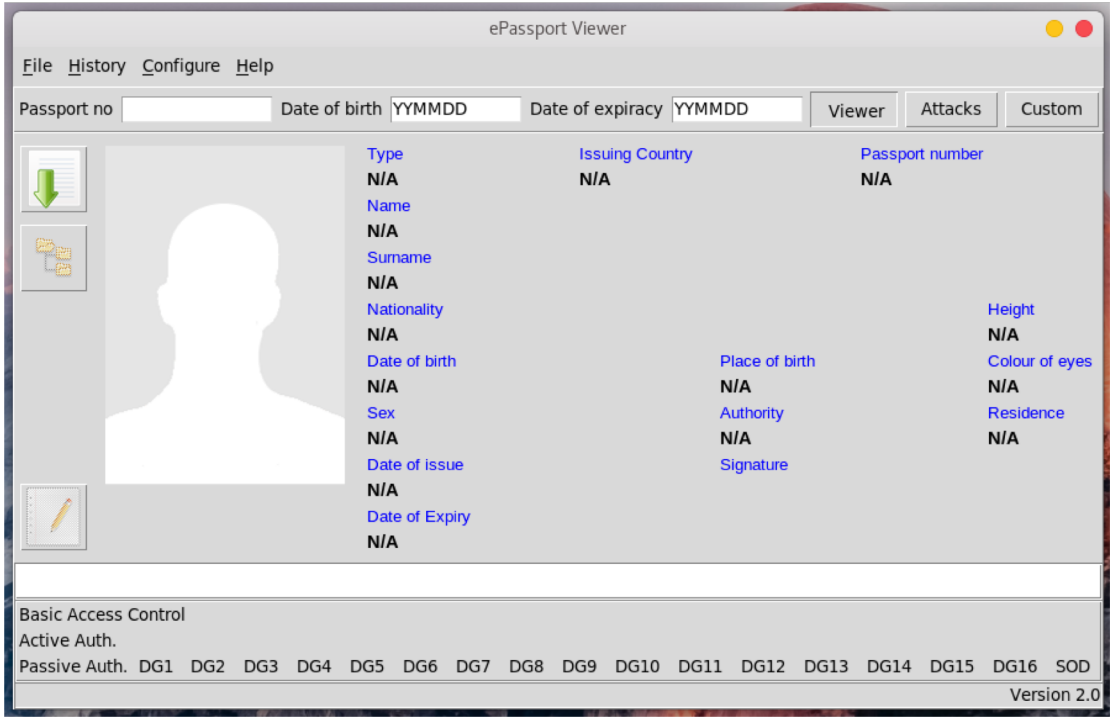
5

ePASSPORT VIEWER

Get your hands dirty

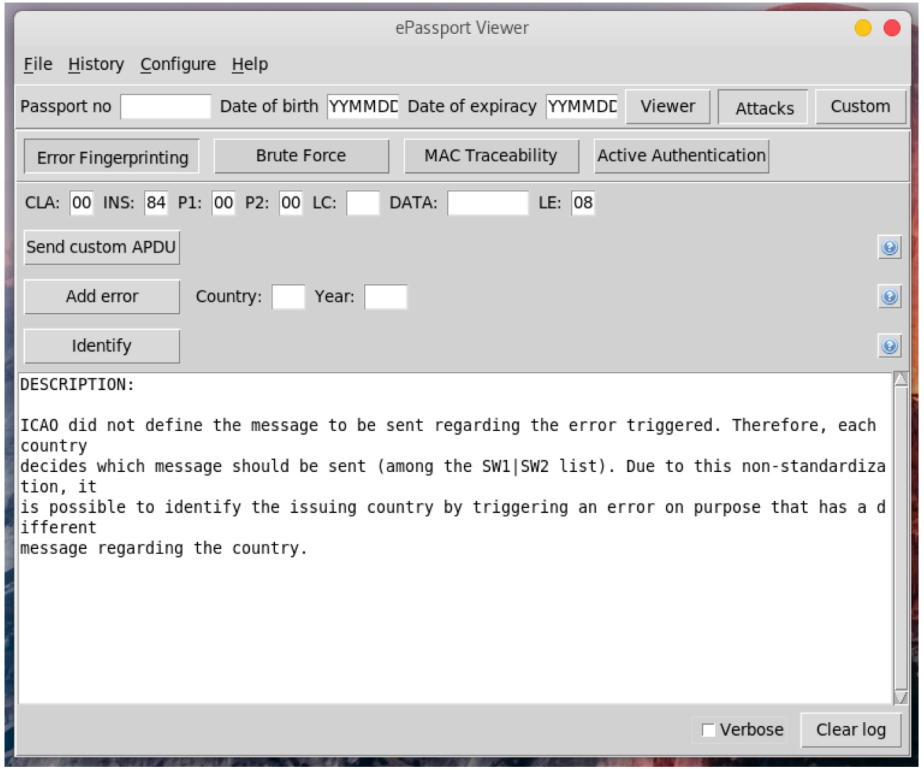
INTERFACE

Read content



INTERFACE

Test attacks



INTERFACE

Communicate with your passport