Biometric Passports

Biometric Systems (DTU 02238)

Christoph Busch

Session 14 and 15

Overview ePassports

Structure of this session

- Motivation for ePassports
- ICAO Specification of Travel Documents
- Passport Content and Logical Data Structure
- Risk Analysis and Countermeasures
- Biometrics and Border Control
- Remaining Challenges

Motivation for ePassports

Passports

Definitions

- Wikipedia: „*A passport is a document, issued by a national government, which certifies, for the purpose of international travel, the identity and nationality of its holder. The elements of identity are name, date of birth, sex, and place of birth.*“
- Bertold Brecht: „*The passport is the most valuable part of a human. It is not so easily created as a human. A human can be created at any place, in a careless manner and without meaningful reason, but never a passport.*“
  (from Flüchtlingsgespräche - B. Brecht)

ICAO Specification of Travel Documents

Standardised Travel Documents

ICAO - International Civil Aviation Organisation

- A specialised UN agency (Headquarter Montreal)
- 193 member states
- ICAO’s mandate for standards development
  - The Convention on International Civil Aviation - Doc 7300 signed in December 1944 (“Chicago Convention”)
  - ICAO works to achieve its vision of safe, secure and sustainable development of civil aviation through the cooperation of its Member States

Convention on International Civil Aviation

Convention relative à l'aviation civile internationale

Convenio sobre Aviación Civil Internacional

Конвенция о международной гражданской авиации

International Civil Aviation Organization
Organisation de l'aviation civile internationale
Organización de Aviación Civil Internacional
Международная организация гражданской авиации

- Technical Advisory Group on Traveller Identification Programme (TAG/TRIP)
  - New Technologies Working Group (NTWG)
- Cooperation with International Organisation for Standardisation (ISO/IEC JTC1)
  - SC17 and SC37

ICAO International Specifications

Doc 9303 Structure: 13 parts (in the 2021 edition)

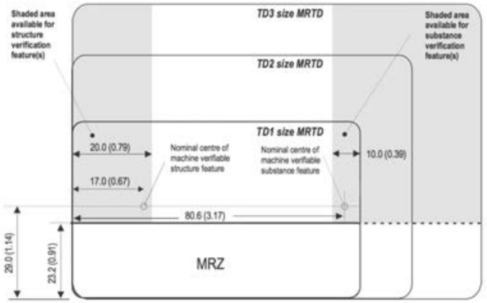
- Part 1 — Introduction
- Part 2 — Specifications for the Security of the Design, Manufacture and Issuance of MRTDs
- Part 3 — Specifications common to all MRTDs
- Part 4 — Specifications for Machine Readable Passports (MRPs) and other TD3 size MRTDs
- Part 5 — Specifications for TD1 size Machine Readable Official Travel Documents (MROTDs)
- Part 6 — Specifications for TD2 size Machine Readable Official Travel Documents (MROTDs)
- Part 7 — Machine Readable Visas
- Part 8 — Emergency Travel Documents
- Part 9 — Deployment of Biometric Identification and Electronic Storage of Data in MRTDs
- Part 10 — Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)
- Part 11 — Security Mechanisms for MRTDs
- Part 12 — Public Key Infrastructure for MRTDs
- Part 13 — Visible Digital Seal (VDS)

ICAO International Specifications

Doc 9303: relevant parts

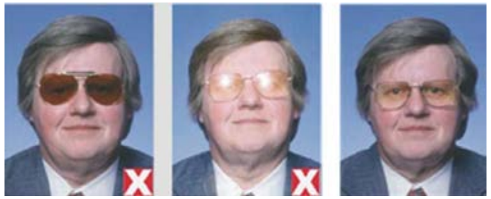
Part 2: Specification for the Security of the Design

MRTD environment: design, production, issuance


Shaded area available for structure verification feature(s)
TD3 size MRTD
Shaded area available for substance verification feature(s)
TD2 size MRTD
TD1 size MRTD
20.0 (0.79)
Nominal centre of machine verifiable structure feature
Nominal centre of machine verifiable substance feature
10.0 (0.39)
17.0 (0.67)
80.6 (3.17)
29.0 (1.14)
23.2 (0.91)
MRZ

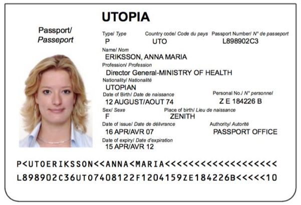
Part 3: Specifications Common to all MRTDs

physical characteristics, visual zone, MRZ, conventions, face image



Part 4: TD3 size MRTDs electronic Passports (MRP)

MRP data page (design and data fields), primary identifier, check digits



UTOPIA

Passport/ *Passeport*

Type/ *Type* P — Country code/ *Code du pays* UTO — Passport Number/ *N° de passeport* L898902C3

Name/ *Nom*
ERIKSSON, ANNA MARIA

Profession/ *Profession*
Director General-MINISTRY OF HEALTH

Nationality/ *Nationalité*
UTOPIAN

Date of Birth/ *Date de naissance* 12 AUGUST/AOUT 74 — Personal No./ *N° personnel* Z E 184226 B

Sex/ *Sexe* F — Place of birth/ *Lieu de naissance* ZENITH

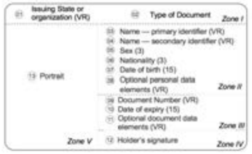
Date of issue/ *Date de délivrance* 16 APR/AVR 07 — Authority/ *Autorité* PASSPORT OFFICE

Date of expiry/ *Date d'expiration*
15 APR/AVR 12

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C36UTO7408122F1204159ZE184226B<<<<<10
```

Part 5:TD1 size MRTDs electronic citizen cards

sequence of data elements, truncation rules



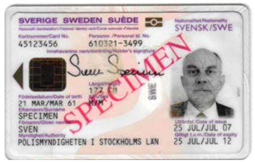
01 Issuing State or organization (VR) — 02 Type of Document — Zone I

03 Name — primary identifier (VR)
04 Name — secondary identifier (VR)
05 Sex (3)
06 Nationality (3)
07 Date of birth (15)
08 Optional personal data elements (VR) — Zone II

13 Portrait

09 Document Number (VR)
10 Date of expiry (15)
11 Optional document data elements (VR) — Zone III

Zone V — 12 Holder's signature — Zone IV



SVERIGE SWEDEN SUÈDE

Nationalitet/Nationality SVENSK/SWE

Kortnummer/Card No. 45123456 — Personnr. /Personal Id. No. 610321-3499

Innehavarens namnteckning/Holder's signature

Längd/Height 177 CM

Födelsedatum/Date of birth 21 MAR/MAR 61 — Kön/Sex M/M

Efternamn/Surname SPECIMEN

Förnamn/Given name SVEN

Myndighet/Authority POLISMYNDIGHETEN I STOCKHOLMS LÄN

Utfärdat /Date of issue 25 JUL/JUL 07

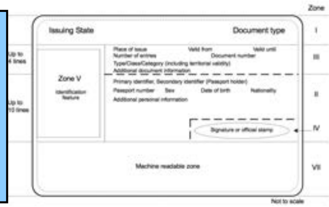
Giltigt t.o.m./Date of expiry 25 JUL/JUL 12

SPECIMEN

SWE

Part 7: Machine Readable Visas (MRV)

specification which allow both visual and machine readable means



Zone

Issuing State — Document type — I

Up to 4 lines — Place of issue, Valid from, Valid until, Number of entries, Document number, Type/Class/Category (including territorial validity), Additional document information — III

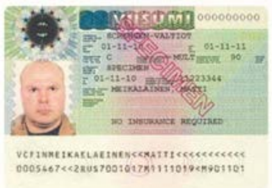
Zone V, Identification feature

Up to 10 lines — Primary identifier, Secondary identifier (Passport holder), Passport number, Sex, Date of birth, Nationality, Additional personal information — II

Signature or official stamp — IV

Machine readable zone — VII

Not to scale



VISUMI 000000000

SCHENGEN-VALTIOT

01-11-10 — 01-11-11

C — MULT — 90

SPECIMEN

01-11-10 — 11223344

MEIKALAINEN, MATTI

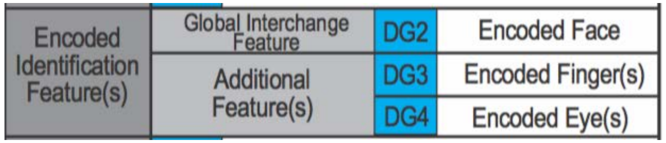
NO INSURANCE REQUIRED

SPECIMEN

```
VCFINMEIKAELAEINEN<<MATTI<<<<<<<<<<<
0005467<<2RUS7001017M1111019<M901101
```

Part 10: Logical Data Structure (LDS)

specification for both visual and mach. readable



Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
	Additional Feature(s)	DG3	Encoded Finger(s)
		DG4	Encoded Eye(s)

Biometrics and ePassports

ICAO - Why biometric data in travel documents?

- Application
  - *Biometric data generated by the enrolment process can be used in a search of one or more biometric databases (identification) to determine whether the end user is known*
  - *When the applicant collects the passport their biometric data can be taken again and verified against the initially captured biometric data*
- Biometrics at the border:
  - *Travellers … can be verified against the reference using the image created at the time the travel document was issued.*
  - *Visually comparing the traveller with the digitised photograph on the Data Page of the traveller’s passport.*

Biometrics and ePassports

- ICAO - New Orleans Resolution - March 2003
  - *“ICAO TAG-MRTD/NTWG recognises that Member States currently and will continue to utilise the facial image as the primary identifier for MRTDs and as such endorses the use of standardised digitally stored facial images as the globally interoperable biometric to support facial recognition technologies for machine assisted identity verification with machine-readable travel documents.*
  - *ICAO TAG-MRTD/NTWG further recognises that in addition to the use of a digitally stored facial image, Member States can use standardised digitally stored fingerprint and/or iris images as an additional globally interoperable biometrics in support of machine assisted verification and/or identification.*
  - *Member States, in their initial deployment of MRTDs with biometrics identifiers, are encouraged to adopt contactless IC media of sufficient capacity to facilitate on-board storage of additional MRTD data and biometric identifiers.”*

Biometrics and ePassports

EU-Council Regulation No 2252/2004 - of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

- Article 1
  - *“Passports issued by Member States to their nationals shall comply with the minimum security standards set out in the Annex.*
  - *Passports and travel documents shall include a storage medium which shall contain a facial image. Member States shall also include fingerprints in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data”*

Biometrics and Identity Cards

Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens

- Reason for and objectives of the proposal
  - *“The inclusion of biometric identifiers, and particularly the inclusion of fingerprints, renders documents more reliable and secure. In that context, it is of crucial importance to phase out documents with weak security features as quickly as possible.“*
  - *“The inclusion of two biometric identifiers (facial image, fingerprints) will improve the identification of persons and align the level of document security of identity cards of EU citizens and residence cards issued to third country family members to the standards of, respectively, passports issued to EU citizens and residence permits issued to third country nationals who are not family members of EU citizens).“*
  - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32019R1157

Passport Content and Logical Data Structure

Biometrics and ePassports

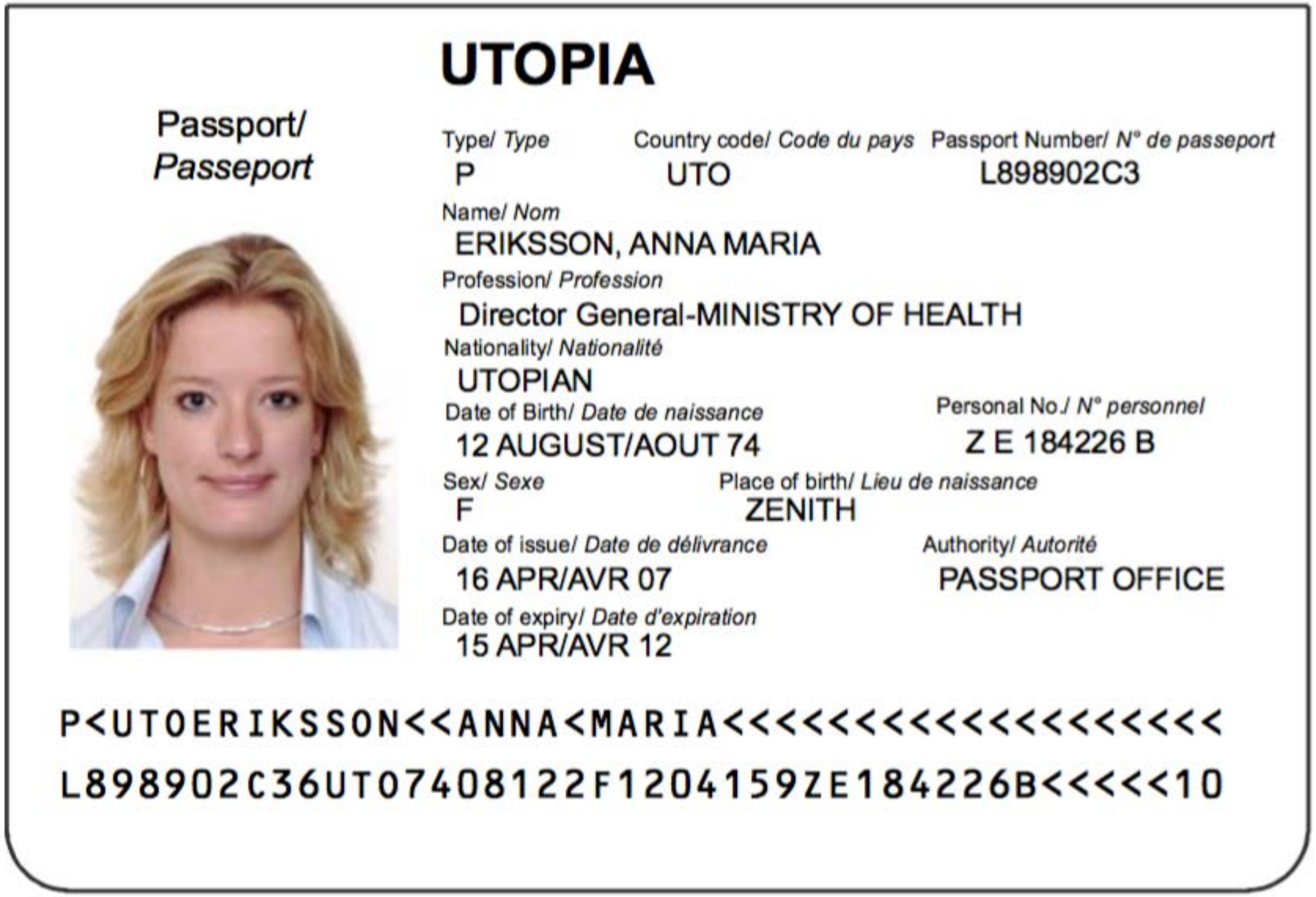
Electronic ICAO 9303 passports

- Contact less IC Chip ISO/IEC14443 (Proximity)
  - minimum 32 Kbyte
- Smart Card OS compliant to ISO/IEC 7816
- Data transmission 8-16 sec
- Logical Data Structure (LDS)
  - info of Machine Readable Zone (MRZ)
  - facial image and fingerprint image
  - electronic signatures
- Validity
  - <25 - 5 years
  - >25 - 10 years (not in all European countries)

ePassport - Data Page

Elements

- Doc type
- Issuing country
- Name
- Doc number
- Nationality
- Date of birth
- Sex
- Date of Expiry
- Check Digits



UTOPIA

Passport/
Passeport

Type/ *Type*	Country code/ *Code du pays*	Passport Number/ *N° de passeport*
P	UTO	L898902C3

Name/ *Nom*
ERIKSSON, ANNA MARIA

Profession/ *Profession*
Director General-MINISTRY OF HEALTH

Nationality/ *Nationalité*
UTOPIAN

Date of Birth/ *Date de naissance*
12 AUGUST/AOUT 74

Personal No./ *N° personnel*
Z E 184226 B

Sex/ *Sexe*
F

Place of birth/ *Lieu de naissance*
ZENITH

Date of issue/ *Date de délivrance*
16 APR/AVR 07

Authority/ *Autorité*
PASSPORT OFFICE

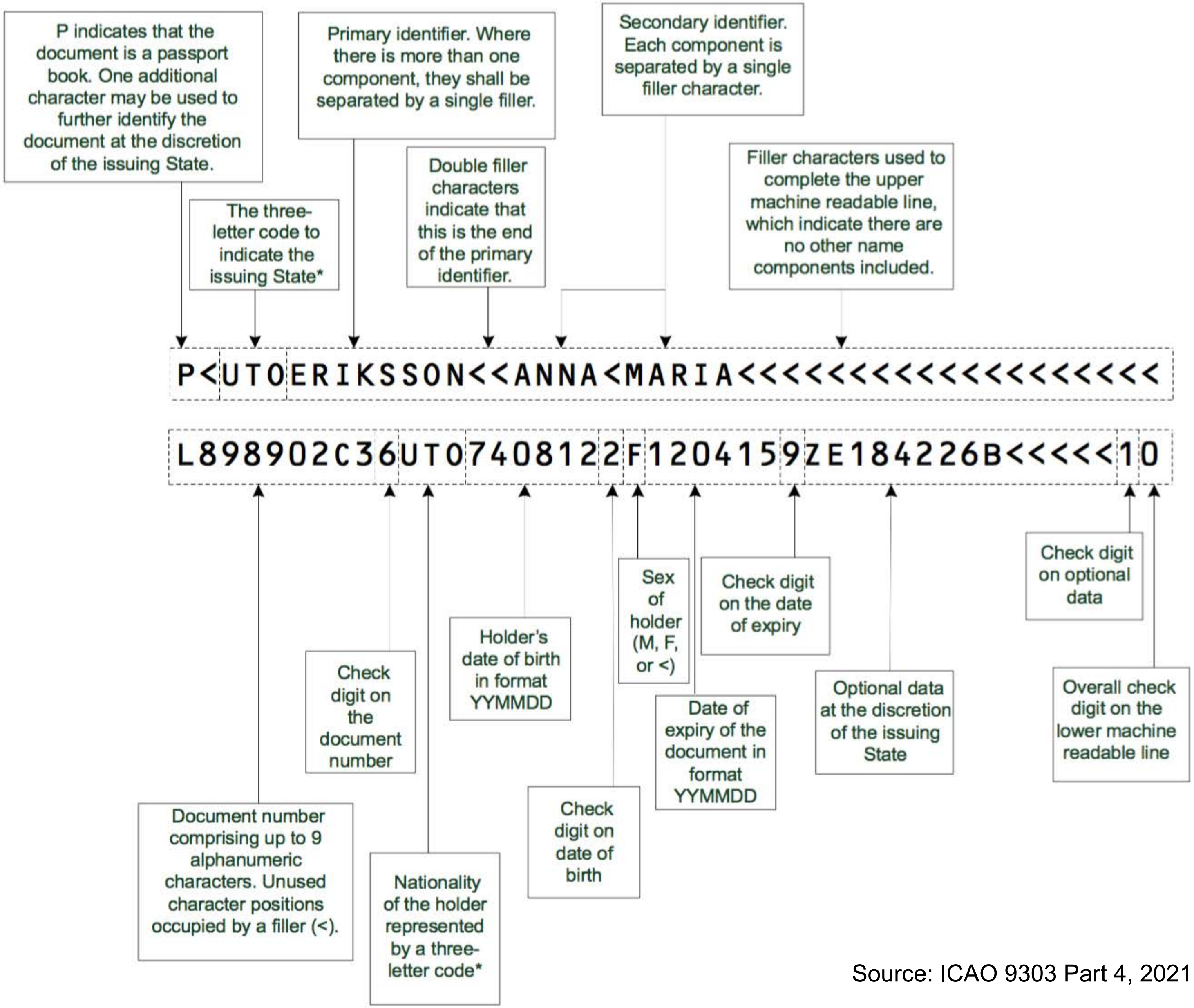
Date of expiry/ *Date d'expiration*
15 APR/AVR 12

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C36UTO7408122F1204159ZE184226B<<<<<10
```

Source: ICAO 9303 Part 4, 2021

ePassport - Data Page

Machine Readable Zone



P indicates that the document is a passport book. One additional character may be used to further identify the document at the discretion of the issuing State.

The three-letter code to indicate the issuing State*

Primary identifier. Where there is more than one component, they shall be separated by a single filler.

Double filler characters indicate that this is the end of the primary identifier.

Secondary identifier. Each component is separated by a single filler character.

Filler characters used to complete the upper machine readable line, which indicate there are no other name components included.

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C36UTO7408122F1204159ZE184226B<<<<<10
```

Document number comprising up to 9 alphanumeric characters. Unused character positions occupied by a filler (<).

Check digit on the document number

Nationality of the holder represented by a three-letter code*

Holder's date of birth in format YYMMDD

Check digit on date of birth

Sex of holder (M, F, or <)

Date of expiry of the document in format YYMMDD

Check digit on the date of expiry

Optional data at the discretion of the issuing State

Check digit on optional data

Overall check digit on the lower machine readable line

Source: ICAO 9303 Part 4, 2021

ePassport Data Group Details

Data stored on the chip (LDS)

- DG1: Information printed on the data page
- DG2: Facial image of the holder (mandatory)

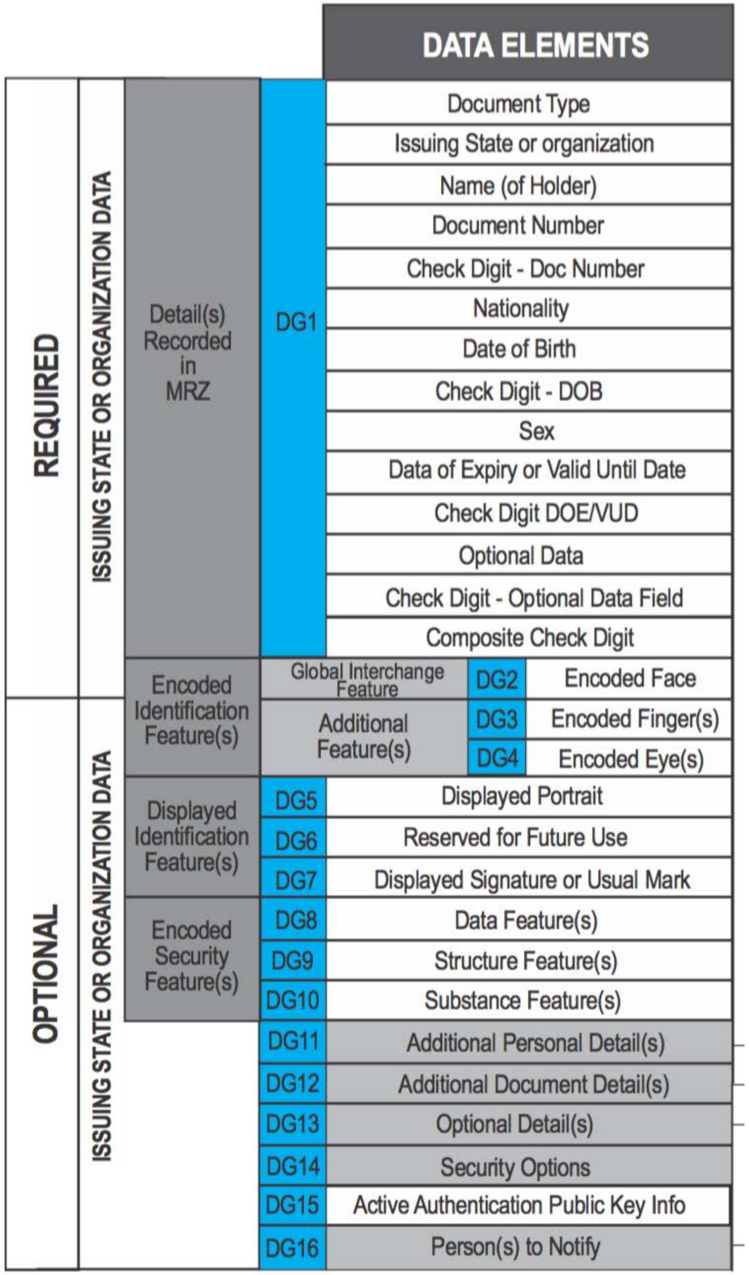
- DG3: Fingerprint image of left and right index finger
- DG4: Iris image (not in the EU)

....

- DG15: Active Authentication Public Key Info
- DG16: Persons to notify

Document Security Object

- Hash values of DGs



					DATA ELEMENTS
REQUIRED	ISSUING STATE OR ORGANIZATION DATA	Detail(s) Recorded in MRZ		DG1	Document Type
					Issuing State or organization
					Name (of Holder)
					Document Number
					Check Digit - Doc Number
					Nationality
					Date of Birth
					Check Digit - DOB
					Sex
					Data of Expiry or Valid Until Date
					Check Digit DOE/VUD
					Optional Data
					Check Digit - Optional Data Field
					Composite Check Digit
		Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
OPTIONAL	ISSUING STATE OR ORGANIZATION DATA		Additional Feature(s)	DG3	Encoded Finger(s)
				DG4	Encoded Eye(s)
		Displayed Identification Feature(s)		DG5	Displayed Portrait
				DG6	Reserved for Future Use
				DG7	Displayed Signature or Usual Mark
		Encoded Security Feature(s)		DG8	Data Feature(s)
				DG9	Structure Feature(s)
				DG10	Substance Feature(s)
				DG11	Additional Personal Detail(s)
				DG12	Additional Document Detail(s)
				DG13	Optional Detail(s)
				DG14	Security Options
				DG15	Active Authentication Public Key Info
				DG16	Person(s) to Notify

Source: ICAO 9303 Part 10, 2015

ePassport Details

Data to be stored in the RFID-Chip

- Alpha-numeric data: 5 Kbyte
- Facial image: ISO/IEC 19794-5:2005
  - 12 Kbyte (JPEG, JPEG2000)
- Fingerprint images: ISO/IEC 19794-4:2005
  - 2* 10 Kbyte (JPEG, JPEG2000, WSQ)

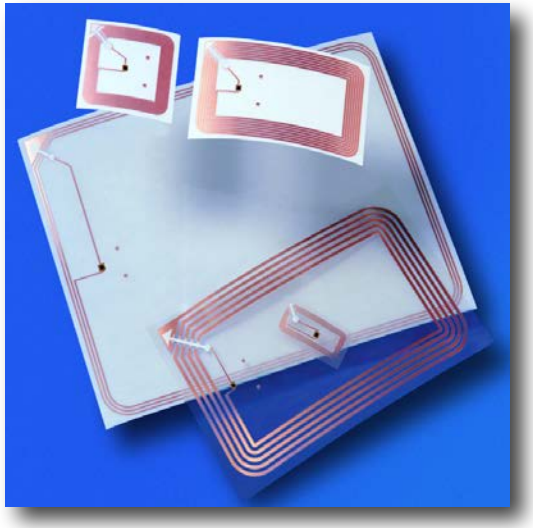
Adopted by ICAO in 2020

- Facial image: ISO/IEC 39794-5:2019
  https://www.iso.org/standard/72155.html
- Fingerprint images: ISO/IEC 39794-4:2019
  https://www.iso.org/standard/72156.html
  - ICAO has adopted its 9303 specification in 2020
    and refers now to ISO/IEC 39794 and its Parts 1, 4 and 5.
  - Passport reader equipment must be able to handle
    ISO/IEC 39794 data by 2025-01-01 (5 years preparation period).
  - Between 2025 and 2030, passport issuers can use the old version
    or the new version of standards (5 years transition period).

ePassport Details

RFID-Chip

- Proximity Integrated Circuit Card (PICC)
- 13,56 MHz
- Readable from 5 - 25 cm
- Passive power consumption



Risk Analysis and Countermeasures

ePassport Properties and Threats

Claimed benefits using the RF-Chip

- Less abrasion -> longer lifetime
- Easier handling

Potential disadvantages using RF-technology

- Potential active or passive attacks
- Privacy risks for the bona fide passport holder
  - Tracking
  - Skimming

Security Requirements

Operator

- Authenticity and Integrity
  - prevention of changes to biometric and personal data
  - writing of data only by authorized organizations
- Copy Protection
  - prevention of copying ePassports
  - close link between chip (electronic data) and the document (visual data)

Passport holder

- Privacy protection
- Confidentiality: access control (who is allowed to read?)
- Guarding of the ommunication

ePassport Security Mechanisms

Data stored on chip is protected by three security mechanisms

	Protection-Goal	Cryptographic Technique	Mechanism
1.)	Authenticity	Digital Signature	Passive Authentication
2.)	Originality	Challenge-Response	Active Authentication
3.)	Confidentiality	Authentication & Secure Channels	Access Control

Mechanism - Passive Authentication

1.) Authenticity - fraud immunity

- In addition to the LDS the chip has a Document Security Object
  - Contains hash representations of the LDS content
  - Signed by the issuing state
- Data Authenticity
  - Being checked by reading devices
- Signing algorithms
  - RSA
  - DSA
  - ECDSA (Elliptic Curve Digital Signature Algorithm)

Mechanism - Passive Authentication

1.) Authenticity - Passport production

- Uses a digital signature to authenticate data stored in the data groups
- This signature is generated by a Document Signer (usually the passport producer) in the personalization phase
- Signature generated over a Document Security Object contains the hash values of all data groups stored on the chip

Mechanism - Passive Authentication

1.) Authenticity - Verification

A terminal has to perform the following steps to verify data stored on a chip:

- Read the Document Security Object from the chip
- Retrieve the corresponding
  - Document Signer Certificate,
  - the trusted Country Signing CA Certificate, and
  - the corresponding Certificate Revocation List
- Verify the Document Signer Certificate and the signature of the Document Security Object
- Compute hash values of all data groups and compare them to the hash values in the Security Object

Security Infrastructure for ePassports

Country Signing PKI:

- Exactly one Root-CA per country: Country Signing CA (CSCA)
- CSCA generates certificates for manufacturers of the ePass: Document-Signer-certificate (DS-certificate)
- Document Signer signs data on the ePass
- Reading device can check signatures using DS-certificate

Country Verifying PKI:

- Exactly one Root-CA per country: Country Verifying CA (CVCA)
- CVCA generates certificates for operators of reading devices: Document-Verifier-certificate (DV-certificate)
- ePass can check authenticity of the reading device using DV-certificate

Mechanism - Active Authentication

2.) Prevent Cloning

- Digital security feature that prevents cloning by introducing a chip-individual key pair:
  - the public key is stored in data group DG15
  - the corresponding private key is stored in secure memory and may only be used internally by the chip and cannot be read out
- The chip can prove knowledge of this private key in a challenge-response protocol, which is called Active Authentication

Mechanism - Active Authentication

2.) Prevent Cloning

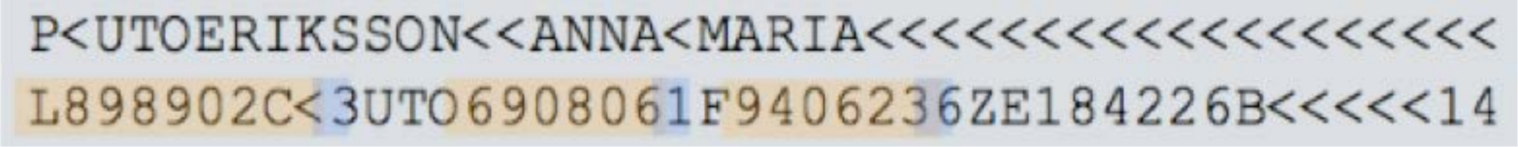
- A terminal has to perform the following steps to verify originality of a chip:
  - generate a random number n
  - let the chip sign this random number n
  - check the signature by using the public key stored in DG15

Mechanism - Access Control

3.a) Basic Access Control (BAC)

Check that the inspection system has physical access

- The inspection system reads the MRZ information consisting of the concatenation of
  - Document-Number, Date-of-Birth and Date-of-Expiry, including their respective check digits

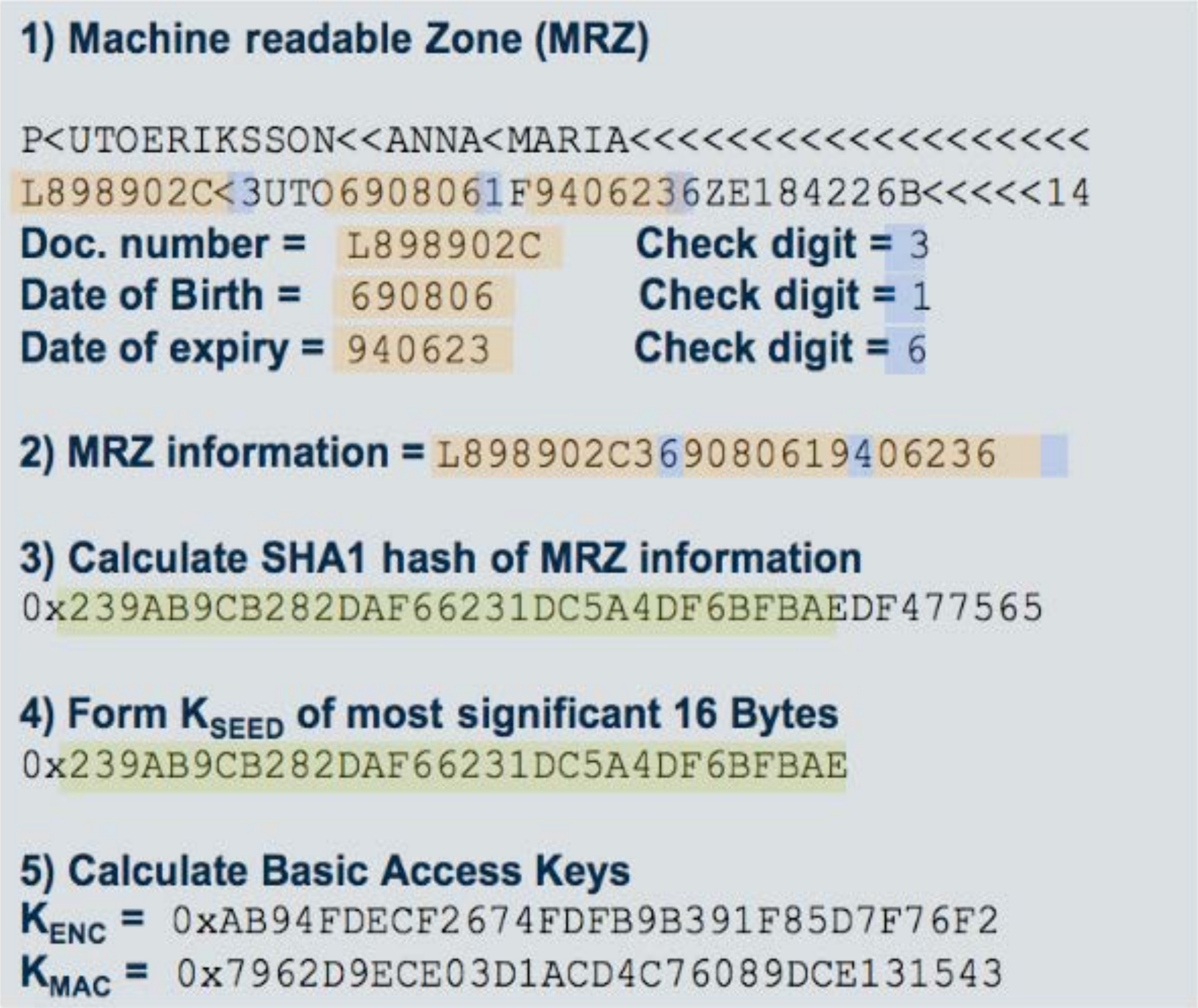


```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```

  - using an OCR-B reader.
  - for a 10 year old document the entropy is 56 bits at maximum
- The most significant 16 bytes of the SHA-1 hash of this MRZ information is used as key seed to derive the Document Basic Access Keys using the key derivation mechanism.
- The inspection system and the MRTD chip mutually authenticate and derive session keys.

Mechanism - Access Control

3.a) Basic Access Control (BAC)



1) Machine readable Zone (MRZ)

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```

Doc. number =	L898902C	**Check digit =**	3
Date of Birth =	690806	**Check digit =**	1
Date of expiry =	940623	**Check digit =**	6

2) MRZ information = L898902C3690806194062366

3) Calculate SHA1 hash of MRZ information

0x239AB9CB282DAF66231DC5A4DF6BFBAEDF477565

4) Form K_{SEED} of most significant 16 Bytes

0x239AB9CB282DAF66231DC5A4DF6BFBAE

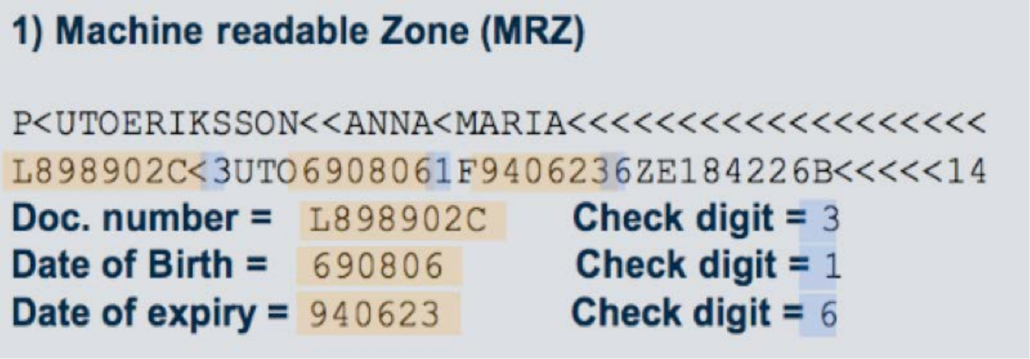
5) Calculate Basic Access Keys

K_{ENC} = 0xAB94FDECF2674FDFB9B391F85D7F76F2

K_{MAC} = 0x7962D9ECE03D1ACD4C76089DCE131543

Mechanism - Access Control

3.a) Check digit control



1) Machine readable Zone (MRZ)

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```

Doc. number = L898902C Check digit = 3

Date of Birth = 690806 Check digit = 1

Date of expiry = 940623 Check digit = 6

	6	9	0	8	0	6
	x	x	x	x	x	x
Weighting:	7	3	1	7	3	1

Step 1 (Multiplication) Product: 42 27 0 56 0 6

Step 2 (Sum of Products) Sum: 42+27+0+56+0+6 **=131**

Step 3 (Division by modulus) 131 mod 10 = 1

Mechanism - Access Control

3.b) Supplemented Access Control (SAC)

- This extended access control allows access to sensitive biometric data (fingerprints, iris, …)
- Aims to grant access only to authorized reading devices
  - both the pass and the reader have to authorize each other
  - only certain countries are granted access to sensitive data
- Reading device has to provide a valid DV-certificate
- Each country's CVCA can limit access to certain data fields using attributes within the DV-certificate

Security Infrastructure for ePassports

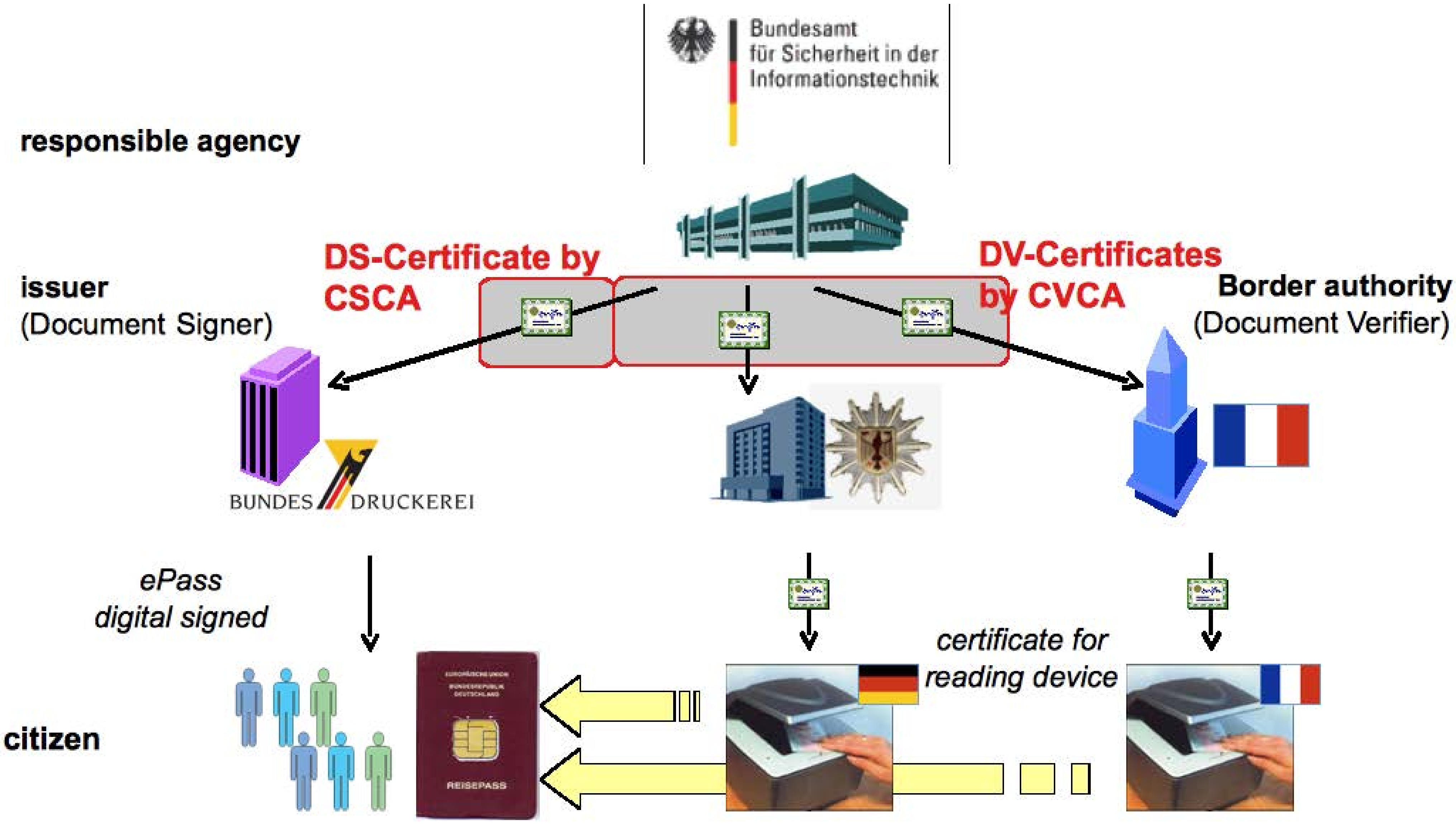
Country Signing PKI:

- Exactly one Root-CA per country:
  Country Signing CA (CSCA)
- CSCA generates certificates for manufacturers of the ePass:
  Document-Signer-certificate (DS-certificate)
- Document Signer signs data on the ePass
- Reading device can check signatures using DS-certificate

Country Verifying PKI:

- Exactly one Root-CA per country:
  Country Verifying CA (CVCA)
- CVCA generates certificates for operators of reading devices: Document-Verifier-certificate (DV-certificate)
- ePass can check authenticity of the reading device using DV-certificate

Security Infrastructure for ePassports

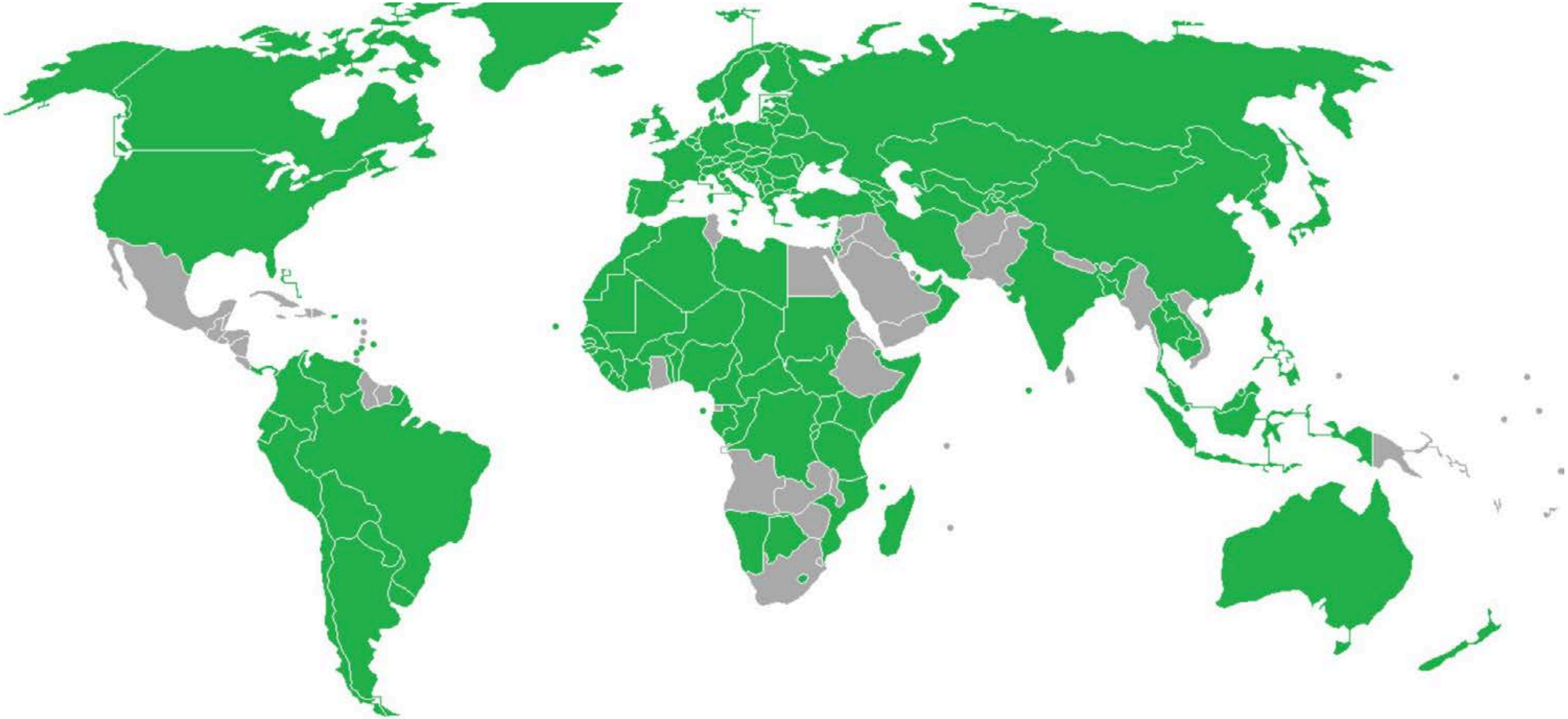


Biometrics and Border Control

Deployment of Biometric Passports

700+ million ePassports

- issued by 112 states (ICAO report as of 2017)



Source:https://en.wikipedia.org/ 2020

Biometrics and Border Control

EU concepts: three categories of travellers

- ePass-Holder (e.g. EasyPASS)
  - citizen of EU/Schengen Country
  - automated, supervised control
    - subject against facial reference in ePassport
- Bona-Fide-Traveller (e.g. EES registration)
  - EU and non-EU frequent traveler
  - intensive control upon registration
  - automated control at border crossing
    - comparison against fingerprints in database
- Third-Country-Traveller
  - non-Bona-Fide-Traveller
  - no automated processing

Biometrics and Border Control (2D Face)

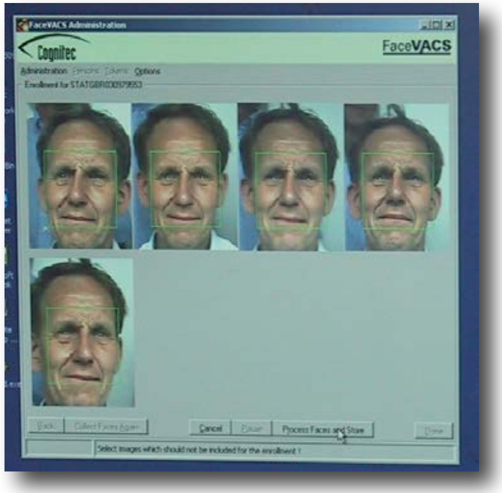
SmartGate - Sydney

- Started in 2003
- FRR due to facial recognition about 2%

Speed Up?

	SmartGate	Manual
Number of travellers	182	16
Minimum time	00:05	00:20
Maximum time	01:32	02:12
Average time	00:17	00:48

Source:Jim Waymann 2004



Enrollment for STATGBR030979853

Select images which should not be included for the enrollment !

Border Control in Frankfurt - EasyPASS

Source: BSI

Automated but supervised Control

- Survey by control personnel

Project goals:

- self-service
  to increase throughput
- Evaluation of face recognition algorithms and usability of ePassport under realistic environment

Operation started 2009

- 4 automated control tracks (Terminal C), 1 monitoring station
- Procedure for travellers
  - no registration needed
  - use of ePassport/Face
  - limited for EU/Schengen-Citizen (18+ years old)

Border Control in Frankfurt - EasyPASS

Operational Figures - as of March 2012

Source: BSI

Source: BSI

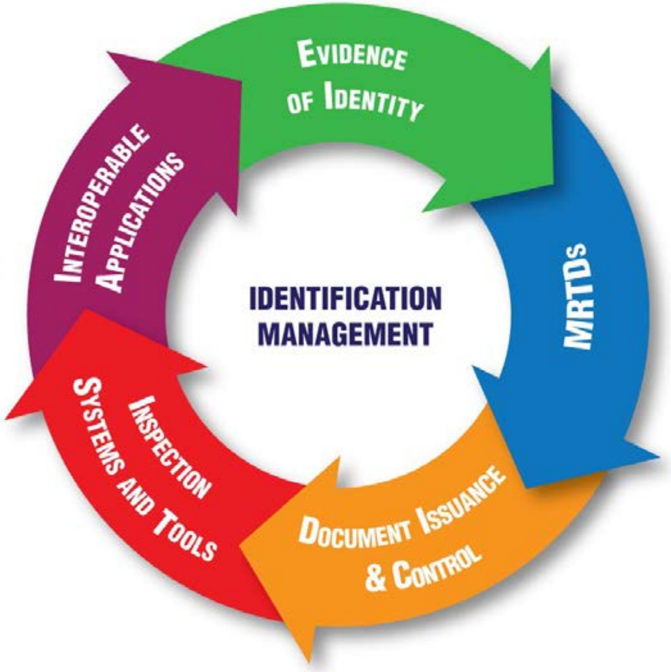
- 88% success rate - no manual interaction needed
- 12% operational reject rate
  - additional manual inspection by border guard
  - approx. 5% rejected due to face verification failed - @0,1%FAR
  - approx. 7% rejected by the system due to other reasons
    - non compliant user behaviour
    - document check failed
    - hits from background database check
- approx. 18 sec average time period to pass the eGate
  - 5-6 sec for reading and checking the ePassport data
  - 5-6 sec for the traveller to enter the eGate
  - 1 sec for biometric verification (face capture and comparison)
  - 5-6 sec for the traveller to leave the eGate

Remaining Challenges

Remaining Challenges

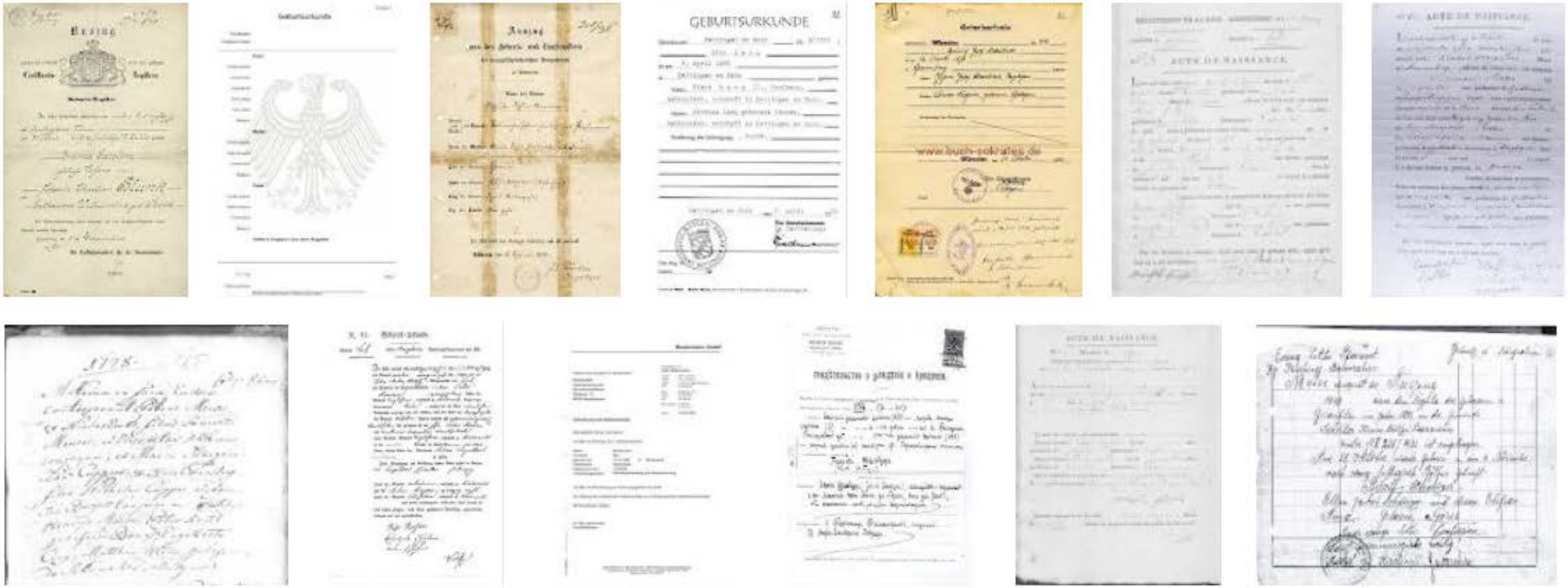
ICAO Traveller Identification Program (TRIP)

- Holistic approach to identification management and travel documents
- Integrates Evidence of Identity, MRTDs, Public Key Directory (PKD) and other dimensions of traveller identification management and border control
- Five dimensions:


EVIDENCE OF IDENTITY
MRTDS
DOCUMENT ISSUANCE & CONTROL
INSPECTION SYSTEMS AND TOOLS
INTEROPERABLE APPLICATIONS
IDENTIFICATION MANAGEMENT

Remaining Challenges

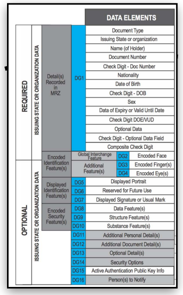
A missing standard for a secure breeder document



Remaining Challenges

Concept of Digital Travel Credentials (DTC)

- Complementing or substituting the passport booklet



					DATA ELEMENTS
REQUIRED	ISSUING STATE OR ORGANIZATION DATA	Detail(s) Recorded in MRZ	DG1		Document Type
					Issuing State or organization
					Name (of Holder)
					Document Number
					Check Digit - Doc Number
					Nationality
					Date of Birth
					Check Digit - DOB
					Sex
					Data of Expiry or Valid Until Date
					Check Digit DOE/VUD
					Optional Data
					Check Digit - Optional Data Field
					Composite Check Digit
		Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
OPTIONAL	ISSUING STATE OR ORGANIZATION DATA		Additional Feature(s)	DG3	Encoded Finger(s)
				DG4	Encoded Eye(s)
		Displayed Identification Feature(s)	DG5		Displayed Portrait
			DG6		Reserved for Future Use
			DG7		Displayed Signature or Usual Mark
		Encoded Security Feature(s)	DG8		Data Feature(s)
			DG9		Structure Feature(s)
			DG10		Substance Feature(s)
			DG11		Additional Personal Detail(s)
			DG12		Additional Document Detail(s)
			DG13		Optional Detail(s)
			DG14		Security Options
			DG15		Active Authentication Public Key Info
			DG16		Person(s) to Notify

Virtual Component (VC)

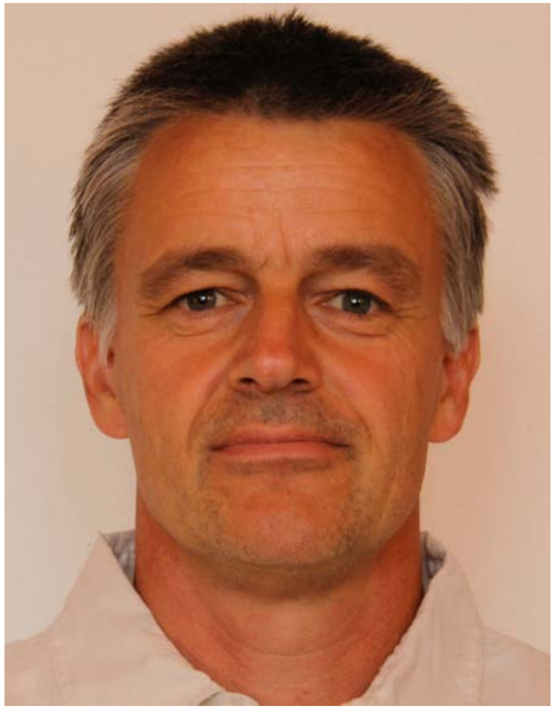
Physical Component (PC)

Physical Component (PC)

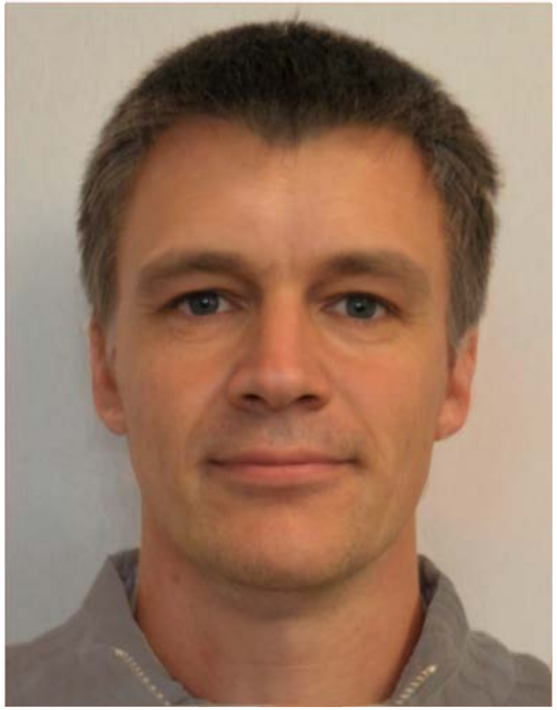
- DTC types
  - eMRTD-PC bound DTC: Passport and additional DTC-PC
  - PC-bound DTC: DTC-V and DTC-PC but no passport

Remaining Challenges

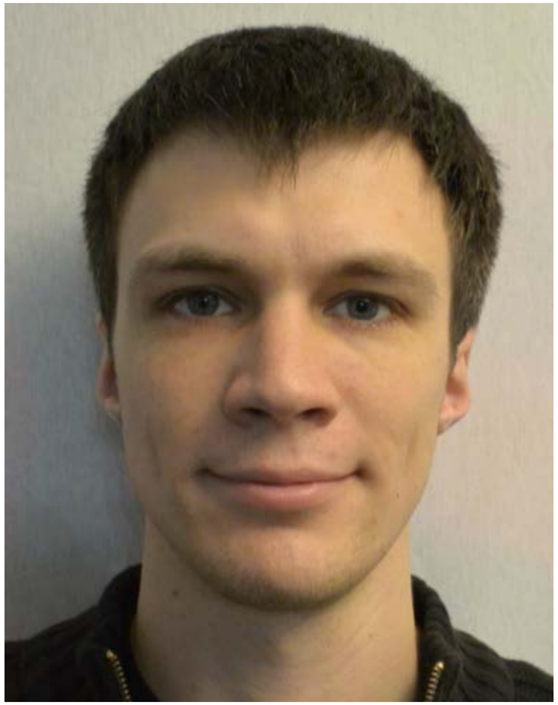
Enrolment attack with morphed facial images



Subject A



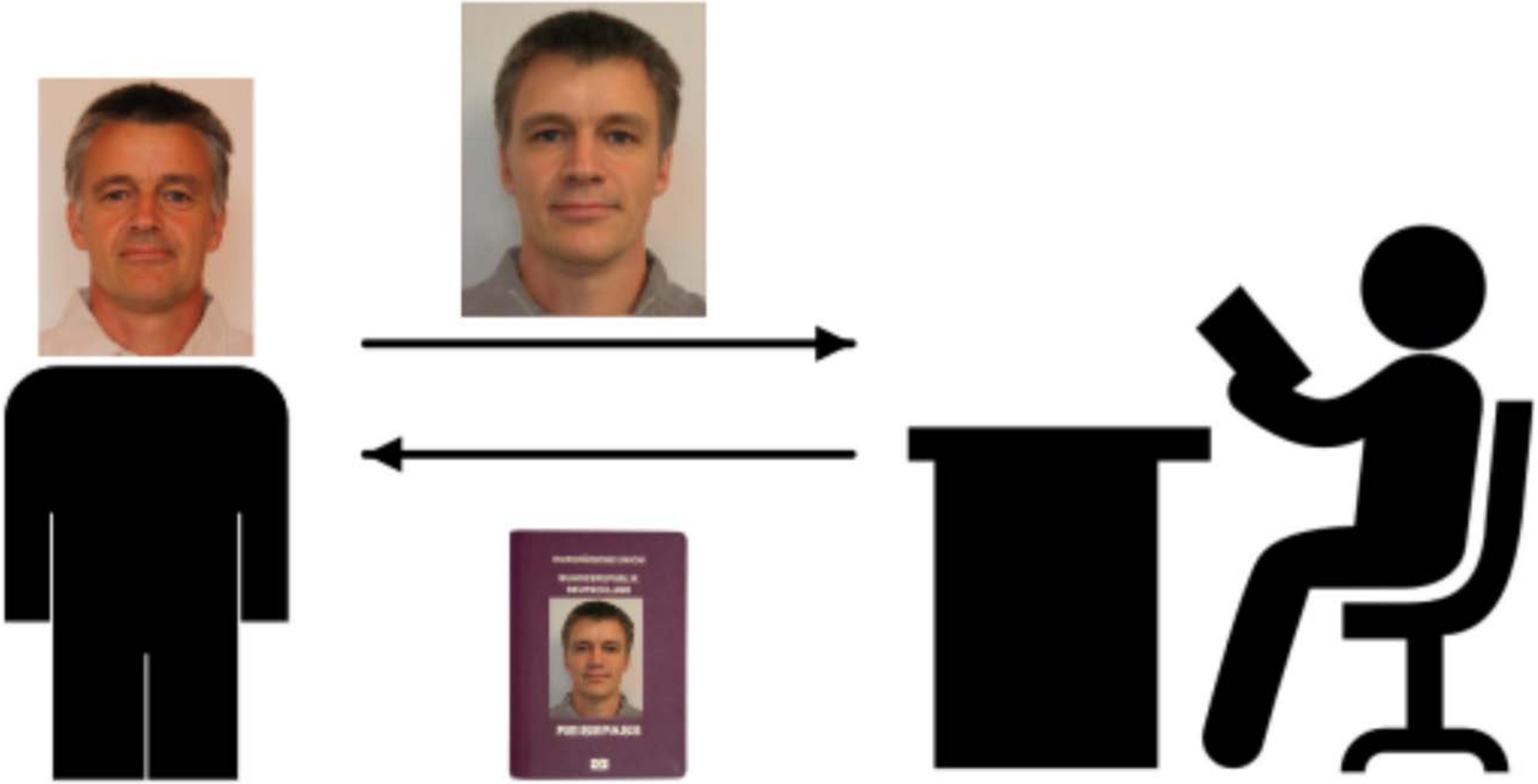
Subject A+B



Subject B

Remaining Challenges

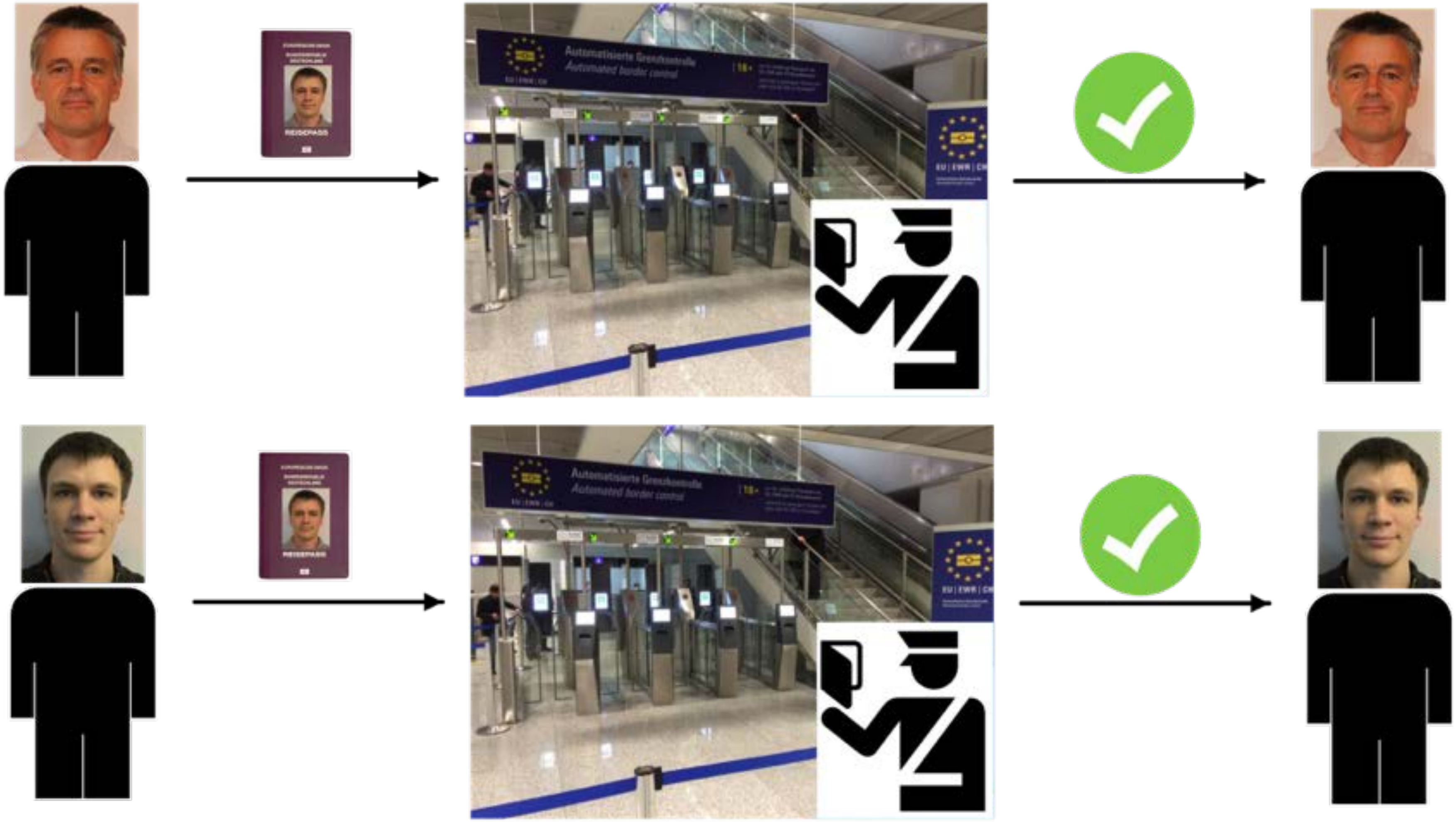
Morphing attack scenario



Challenge: Morphing Attacks

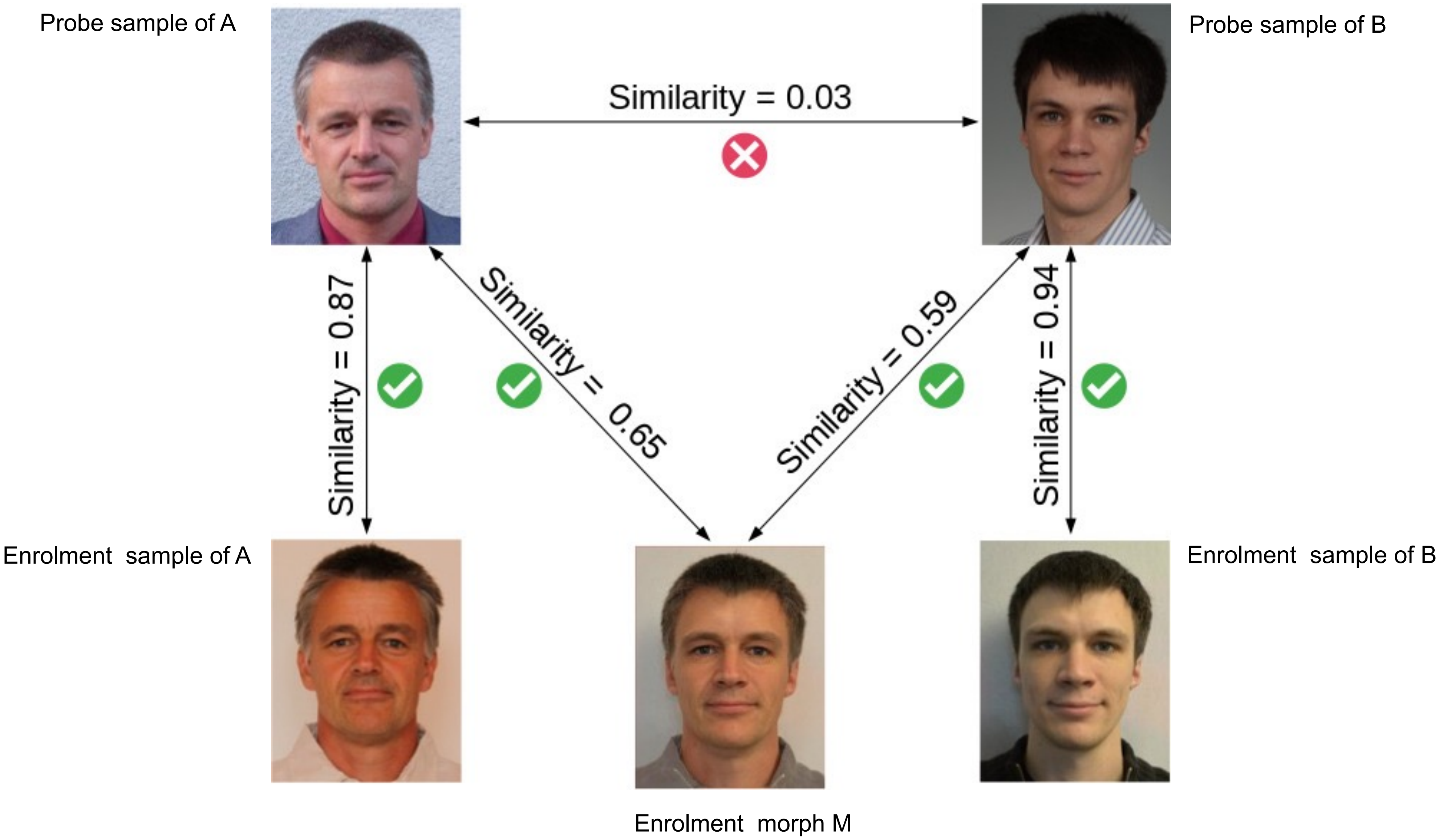
Morphing attack scenario

- Border control



Problem: Morphing Attacks

Verification against morphed facial images



Probe sample of A

Probe sample of B

Similarity = 0.03 ✗

Similarity = 0.87 ✓

Similarity = 0.65 ✓

Similarity = 0.59 ✓

Similarity = 0.94 ✓

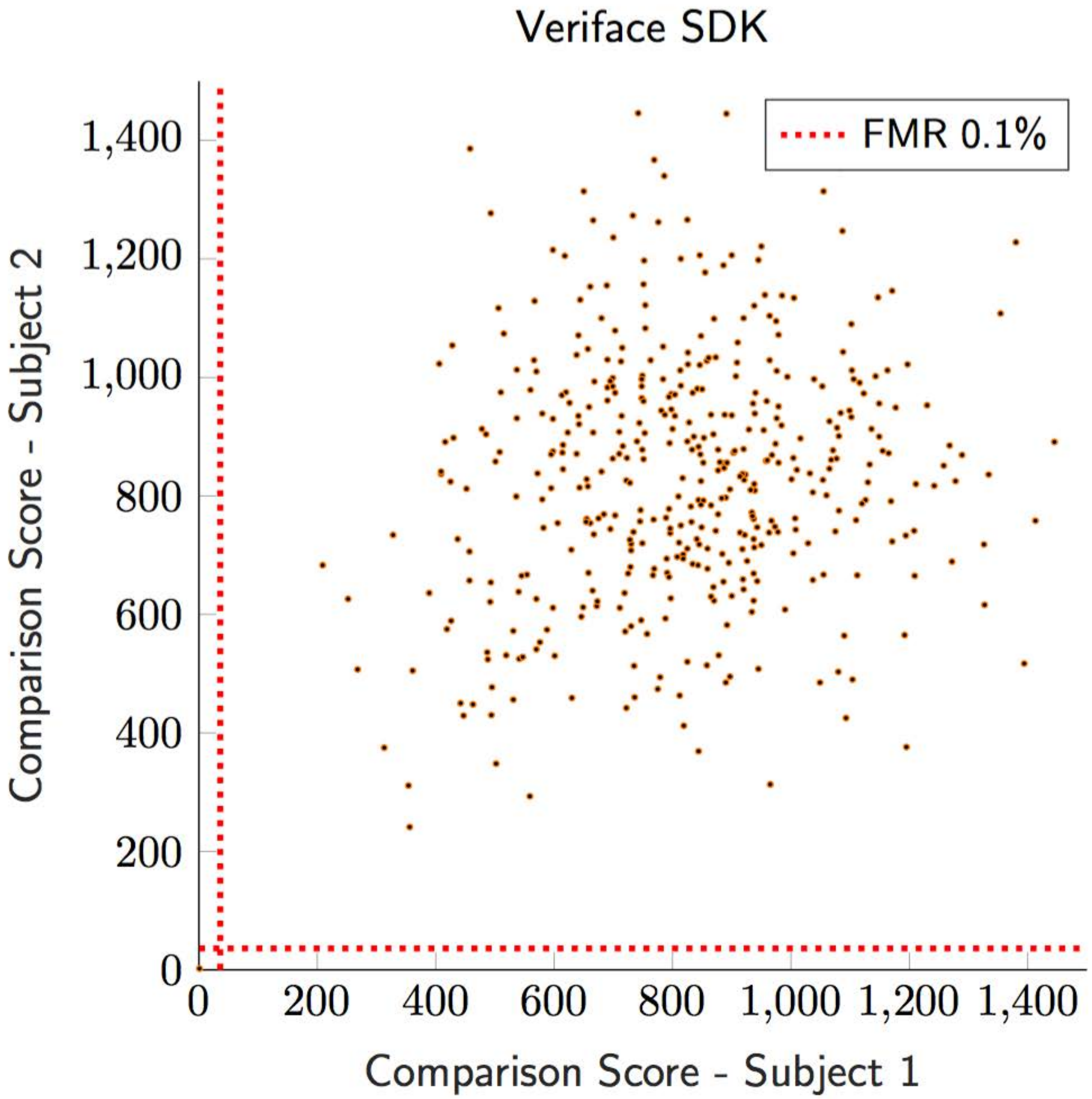
Enrolment sample of A

Enrolment sample of B

Enrolment morph M

Remaining Challenges

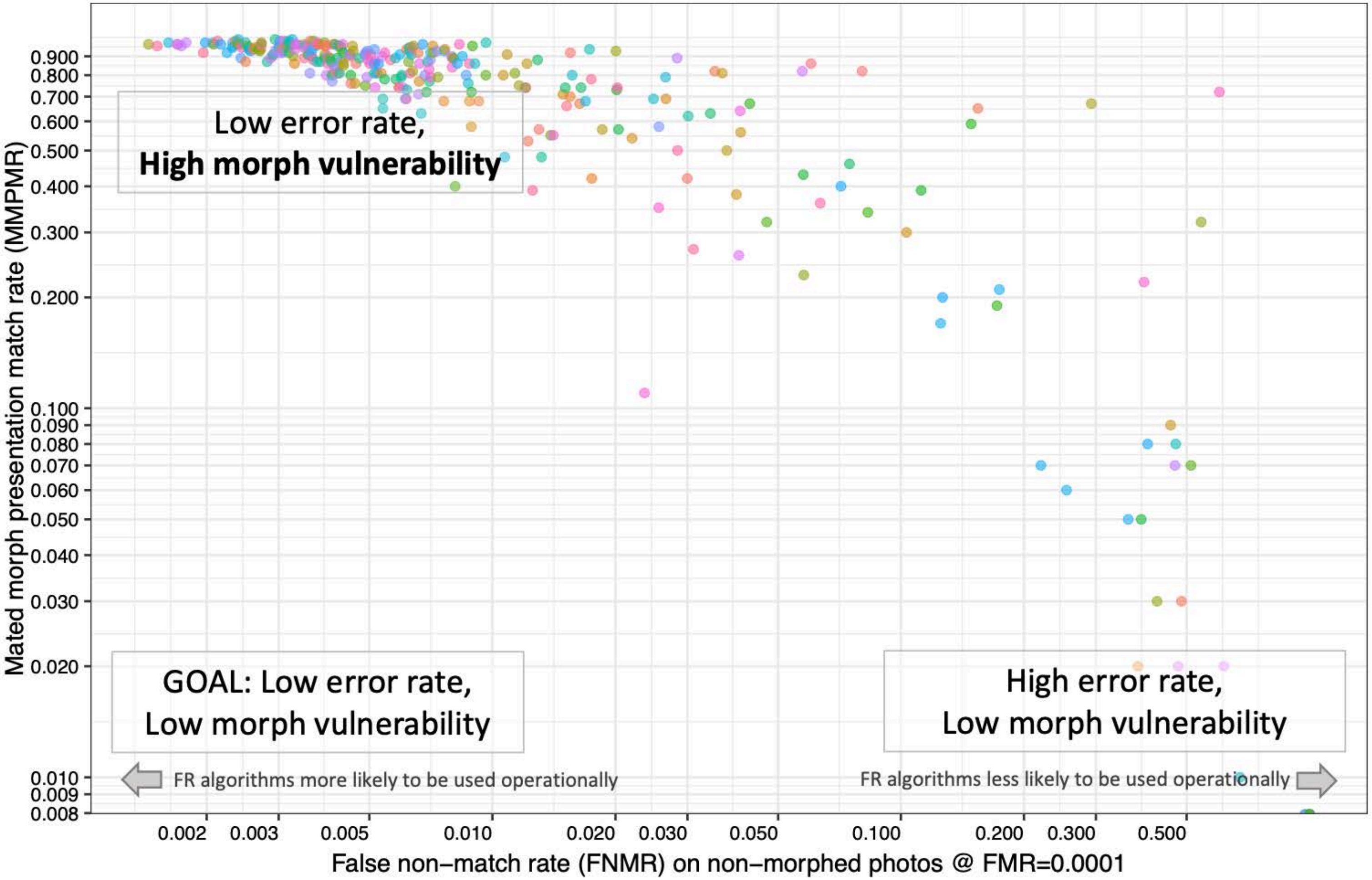
Vulnerability of face recognition to morphing attacks



Scale of the Problem: Vulnerability of FRS

NIST IR 8430 report on FRS vulnerability [Ngan2022]

- Accurate FRS are more vulnerable!

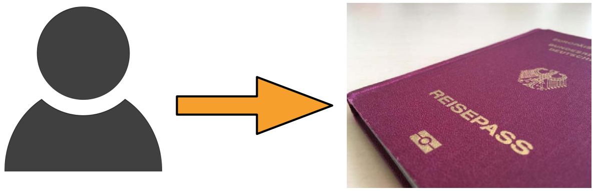


[Ngan2022] NIST IR 8430: "FRVT MORPH: Utility of 1:N Face Recognition Algorithms for Morph Detection“, 2022
https://pages.nist.gov/frvt/reports/morph/frvt_morph_4A_NISTIR_8430.pdf

Unique Link

Principle of equality - in our society

- One individual - one passport



✓

Principle of unique link of ICAO ⚠

- One individual - one passport

image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

Unique Link

Principle of equality - in our society

- One individual - one passport

✓

Principle of unique link of ICAO ⚠

- One individual - one passport
- ICAO 9303 part 2, 2006:
  „***Additional security measures:*** *inclusion of a machine verifiable biometric feature linking the document to its legitimate holder*“

image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

Unique Link

Principle of unique link of ICAO

- One individual - one passport

We don’t want this principle of unique link to be broken

- Multiple individuals - one passport

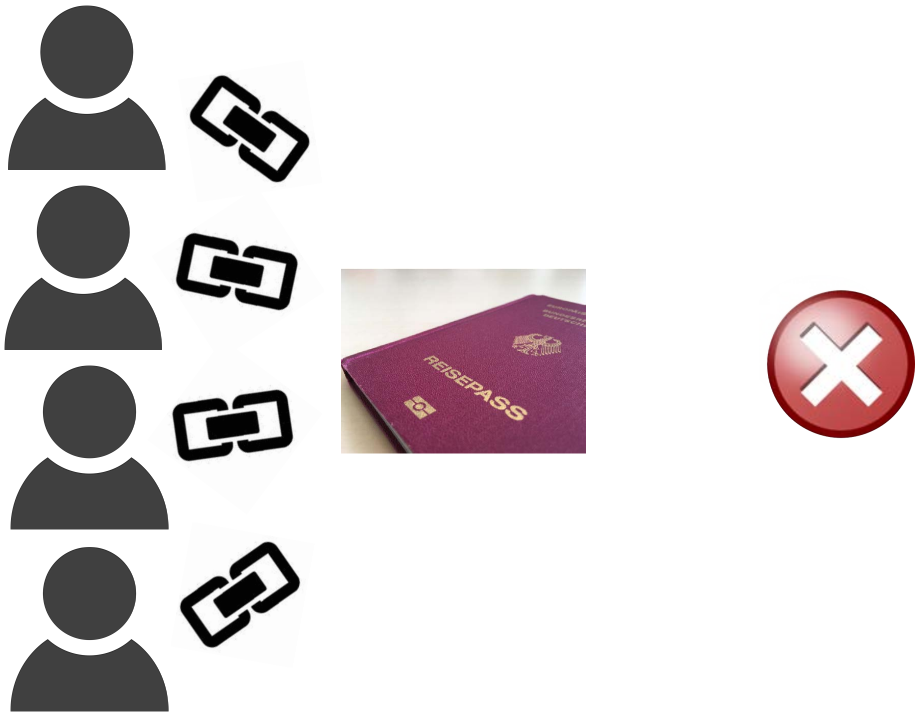
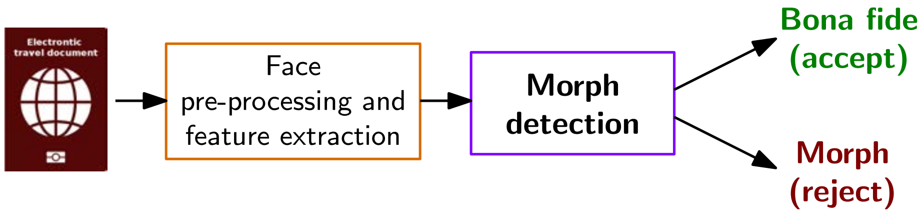


image source: https://pixabay.com/de/vectors/tick-sternchen-kreuz-rot-gr%C3%BCn-40678/

Morphing Attack Detection Scenarios

Real world scenarios

- Single image morphing attack detection (S-MAD)
  - One single facial image is analysed (e.g. in the passport application office)

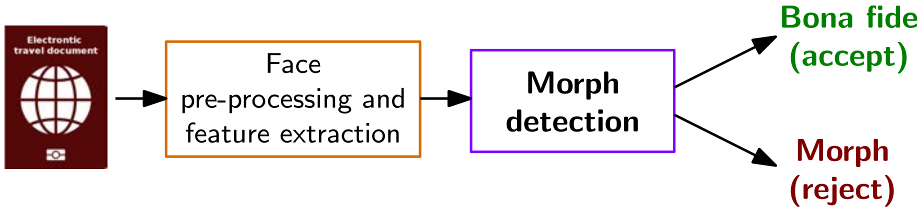

Electrontic travel document
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), April 24-27, (2018)

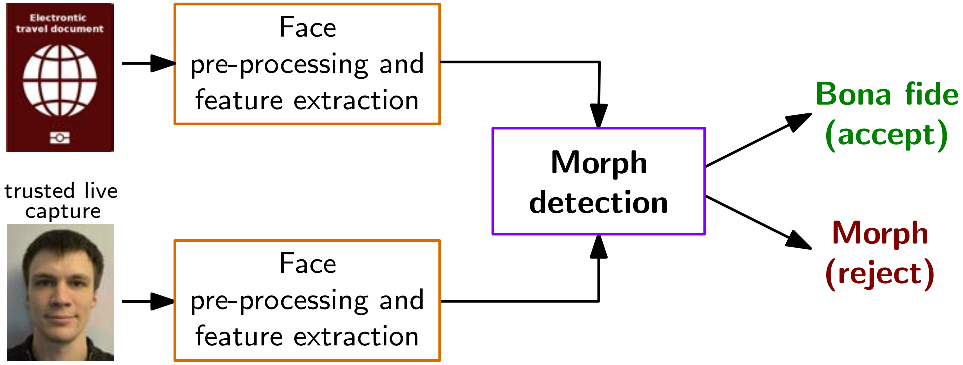
Morphing Attack Detection Scenarios

Real world scenarios

- Single image morphing attack detection (S-MAD)
  - One single facial image is analysed (e.g. in the passport application office)


Electrontic travel document
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

- Differential morphing attack detection (D-MAD)
  - A pair of images is analysed - and one is a trusted Bona Fide image
  - Biometric verification (e.g. at the border)

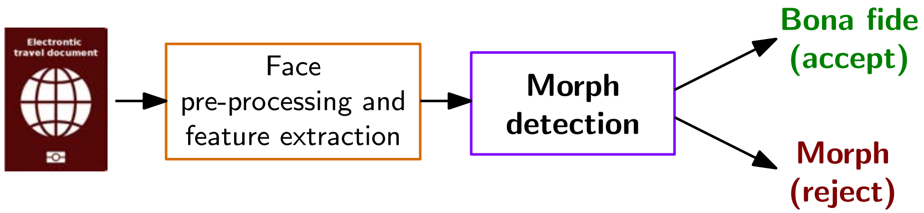

Electrontic travel document
trusted live capture
Face pre-processing and feature extraction
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)

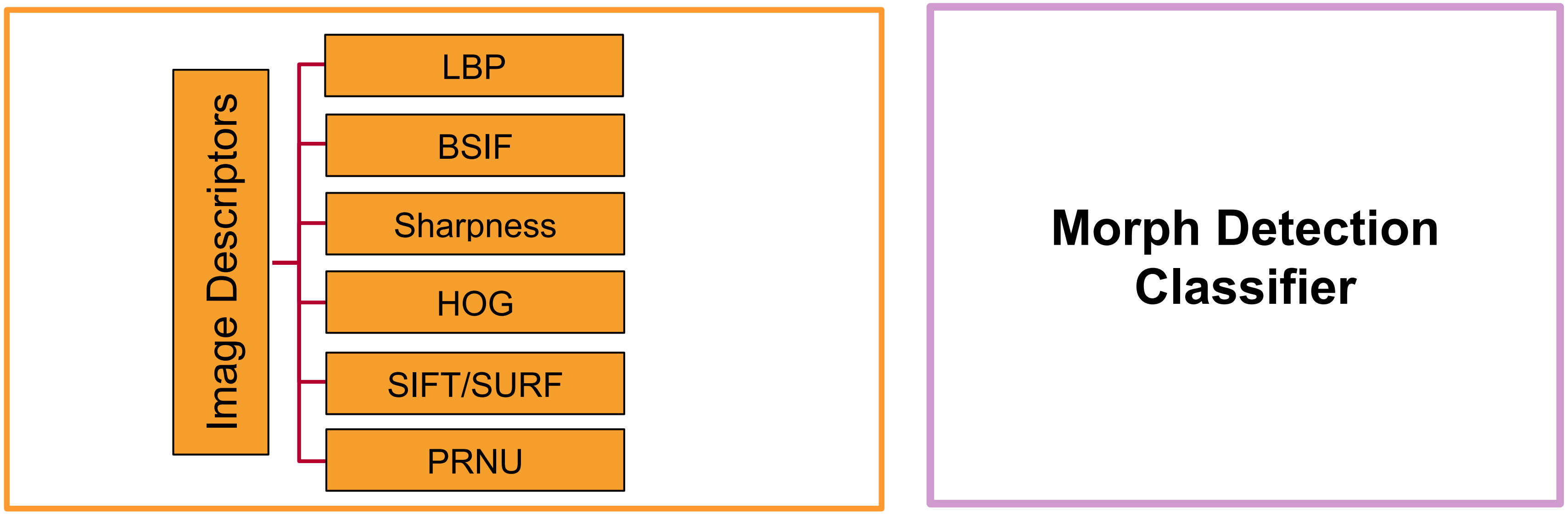
[SRB2018a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), April 24-27, (2018)

Face Pre-processing and Feature Extraction

Morphing Attack Detection (S-MAD) with texture analysis

- Image descriptors as hand-crafted features

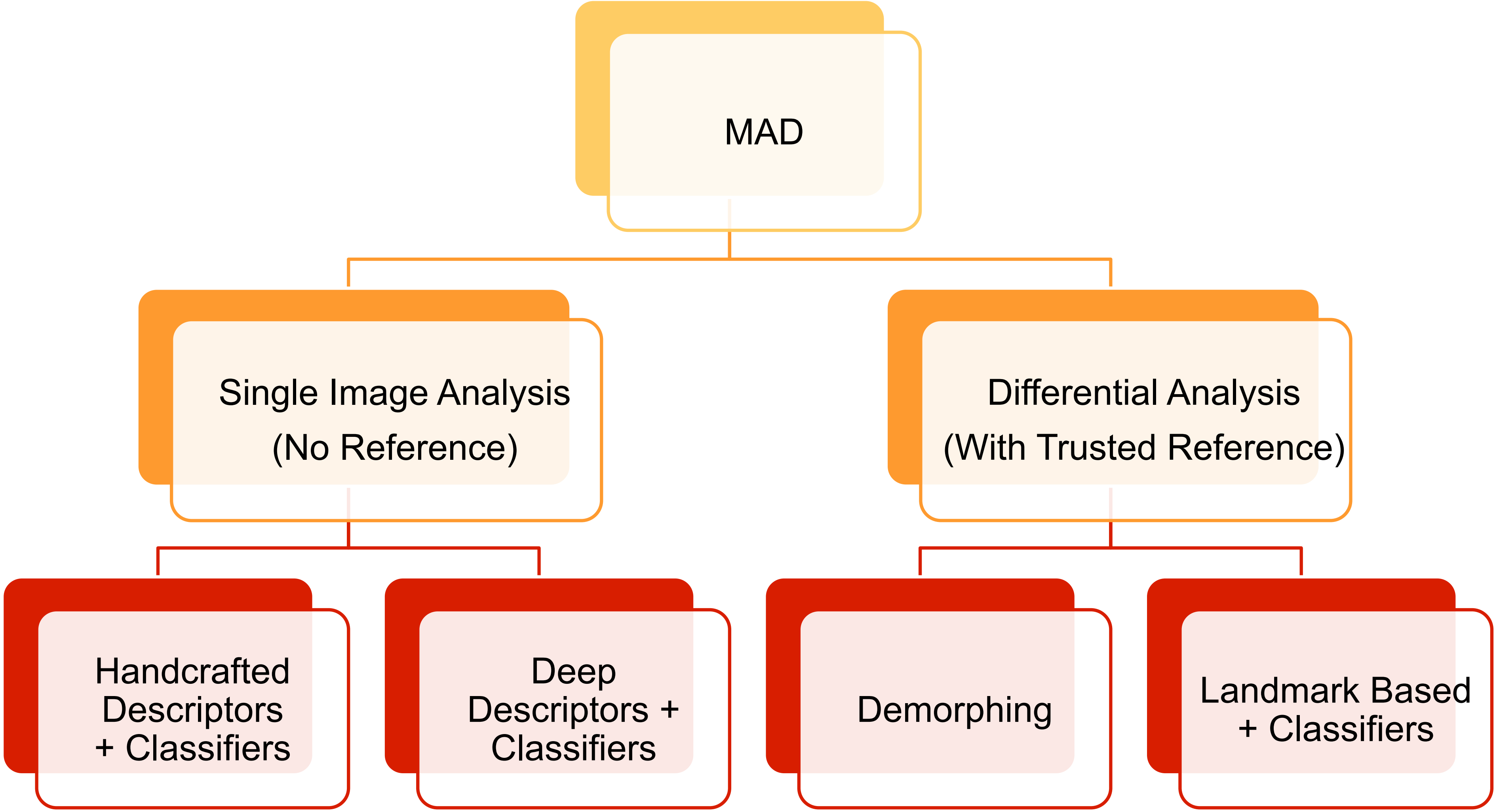

Electrontic travel document
Face pre-processing and feature extraction
Morph detection
Bona fide (accept)
Morph (reject)



[SRB2018b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA 2018), Amsterdam, The Netherlands, May 16-18, (2018)

Summary of MAD Algorithms

Taxonomy of Morphing Attack Detection


MAD
Single Image Analysis (No Reference)
Differential Analysis (With Trusted Reference)
Handcrafted Descriptors + Classifiers
Deep Descriptors + Classifiers
Demorphing
Landmark Based + Classifiers

[SRMBB2019] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Face Recognition Systems under Morphing Attacks: A Survey“, in IEEE Access, (2019)

MAD Evaluation Methodology

Face Morphing Attack evaluations are complex

- Evaluations must consider a dedicated methodology [SNR2017]
- Evaluations must consider many parameters

result = f (dataset-training, dataset-testing, morphing-attack,
landmark-detector, feature-extractor, classifier,
scenario (S-MAD vs. D-MAD),
post-processing, printer, scanner, ageing)

[SNR2017] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, C. Busch: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 20-22, (2017)

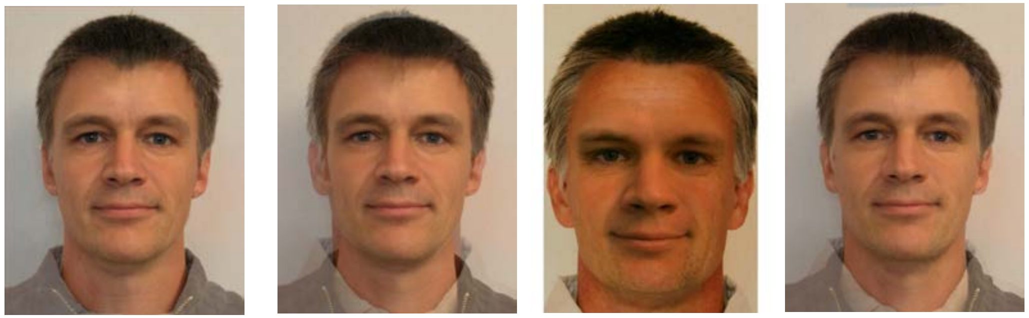
MAD Evaluation

Evaluations must consider many parameters

- Morphing may require manual interaction

result = f (dataset-training, dataset-testing, morphing-attack,
landmark-detector, feature-extractor, classifier,
scenario (S-MAD vs. D-MAD),
post-processing, printer, scanner, ageing)

Automated face morphing tools may introduce artifacts



Fantamorph openCV splicing GIMP

Large set of accessible morphing mechanisms at zero or low cost

- Fantamorph - http://www.fantamorph.com/index.html
- openCV - http://www.learnopencv.com/face-morph-using-opencv-cpp-python
- splicing - http://www.piviandco.com/apps/mixbooth
- GIMP animation package - http://registry.gimp.org/node/18398

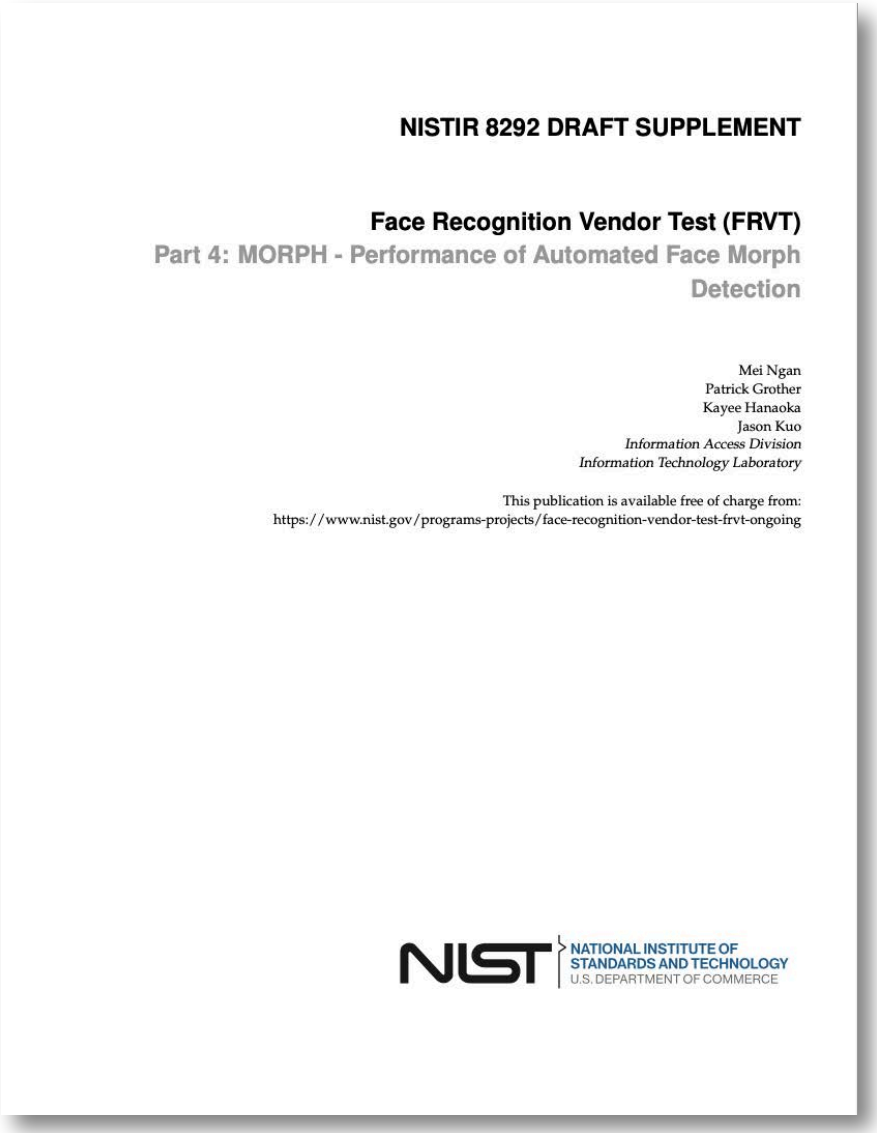
NIST-FRVT-MORPH

NIST IR 8292 report presented March, 2023

FRVT-MORPH

https://pages.nist.gov/frvt/html/frvt_morph.html

- results for MAD algorithms from six research labs:
  - University of Bologna (UBO)
  - Norwegian University of Science and Technology (NTNU)
  - Hochschule Darmstadt (HDA)
  - West Virginia University (WVU)
  - Universidade de Coimbra (VIS)
  - secunet (SEC)



NISTIR 8292 DRAFT SUPPLEMENT

Face Recognition Vendor Test (FRVT)

Part 4: MORPH - Performance of Automated Face Morph Detection

Mei Ngan
Patrick Grother
Kayee Hanaoka
Jason Kuo
Information Access Division
Information Technology Laboratory

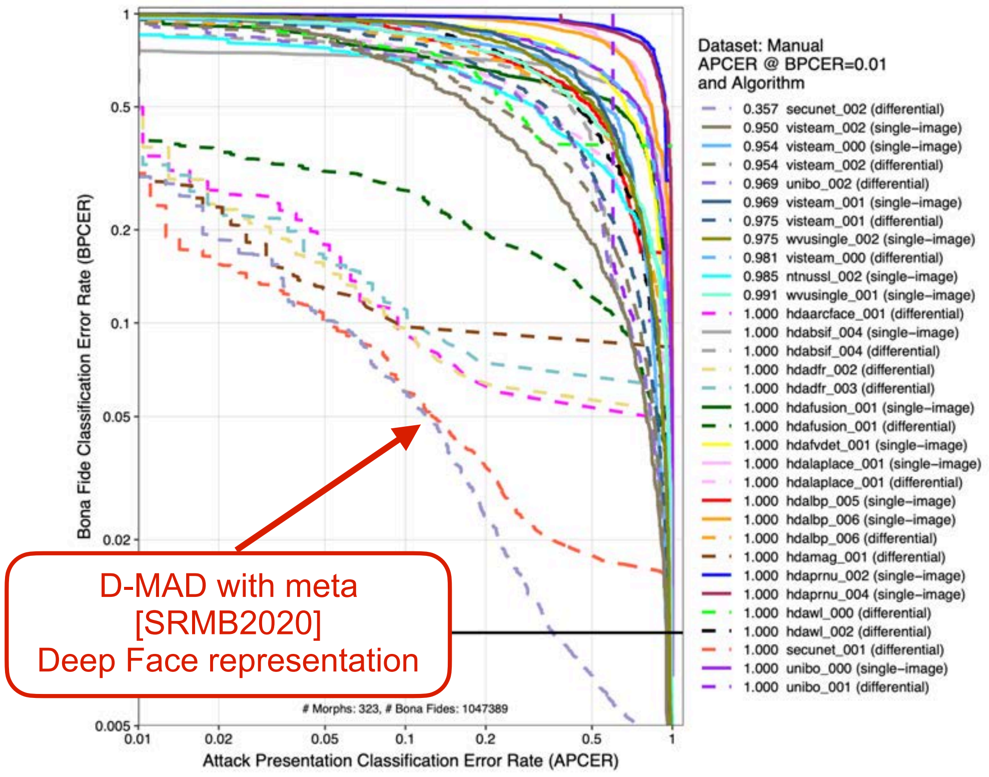
This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

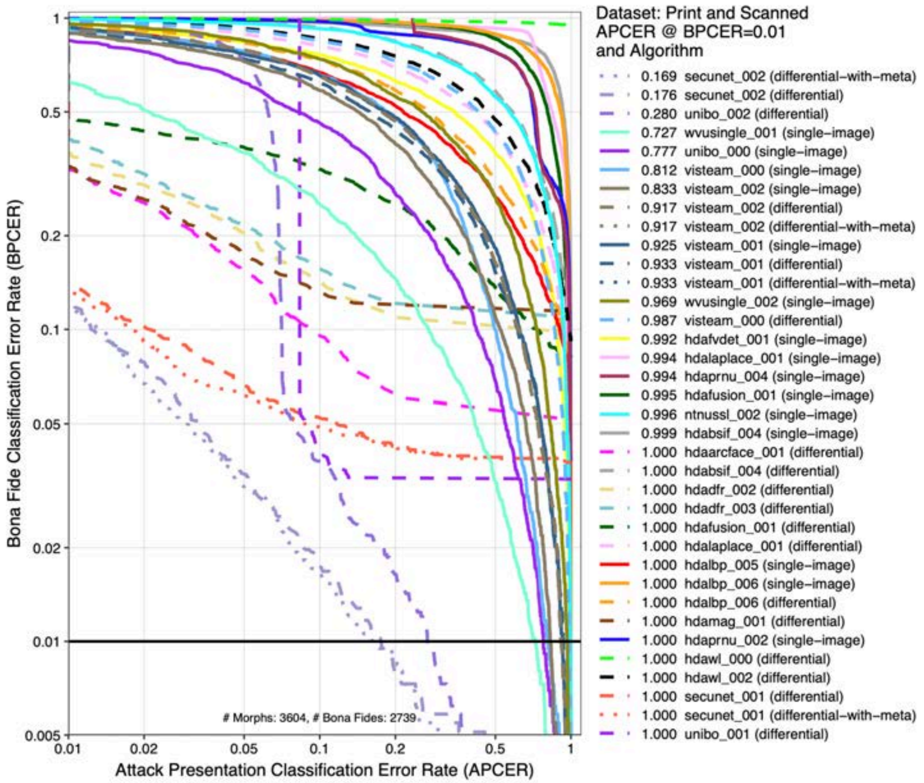
NIST-FRVT-MORPH

NIST IR 8292 report presented March, 2023

- Performance of Automated Face Morph Detection
  https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf
- results for high quality morphs versus print and scanned
  - note the low number of print and scanned images



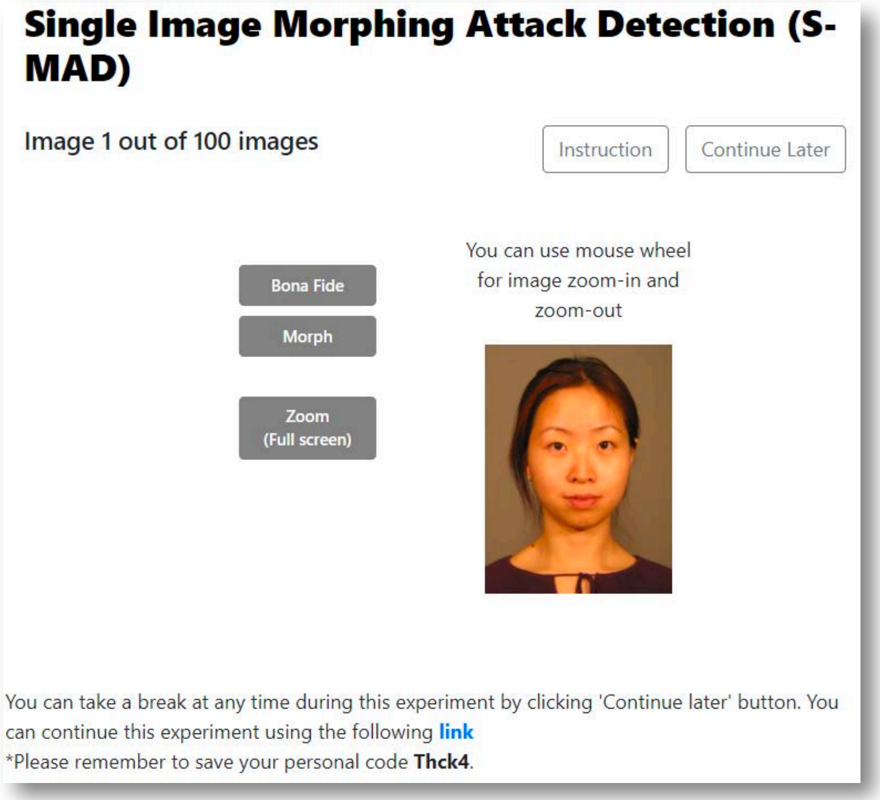
D-MAD with meta
[SRMB2020]
Deep Face representation



Human Experts in MAD

Border guards, case handlers, document examiners, ID experts

- S-MAD: 410 participants, 180 trials
- D-MAD: 469 participants, 400 trials (4 x 100 tasks)



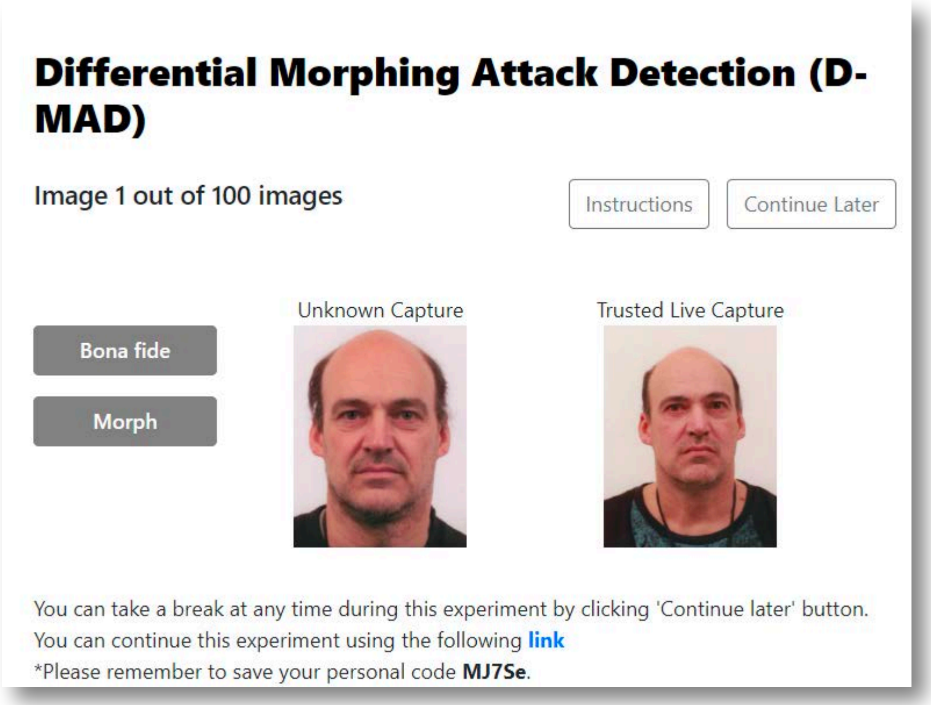
Single Image Morphing Attack Detection (S-MAD)

Image 1 out of 100 images

You can use mouse wheel for image zoom-in and zoom-out

You can take a break at any time during this experiment by clicking 'Continue later' button. You can continue this experiment using the following link

*Please remember to save your personal code **Thck4**.



Differential Morphing Attack Detection (D-MAD)

Image 1 out of 100 images

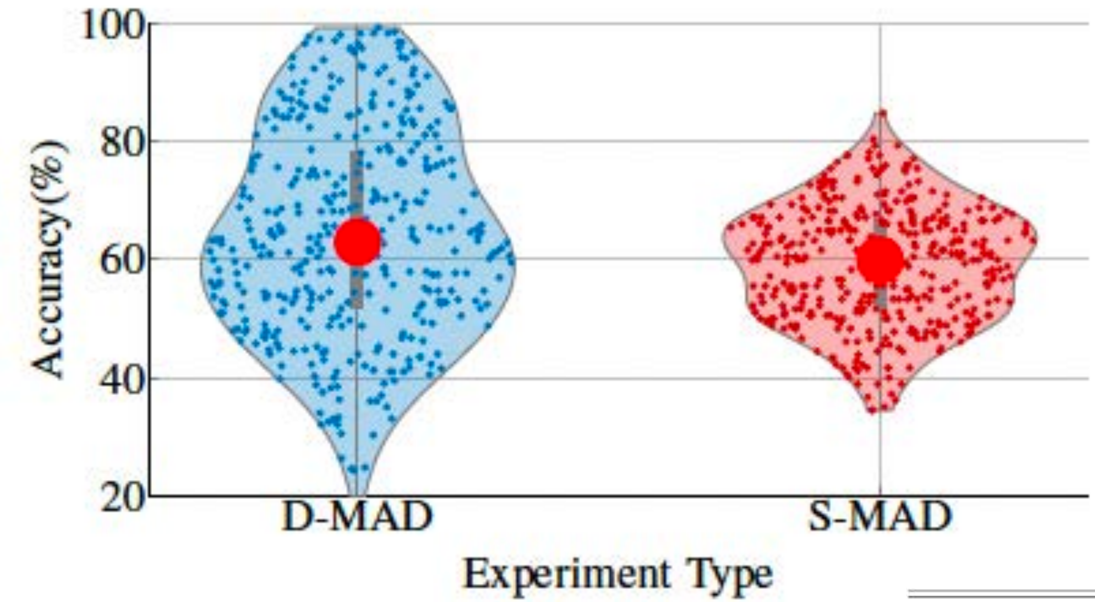
You can take a break at any time during this experiment by clicking 'Continue later' button.
You can continue this experiment using the following link

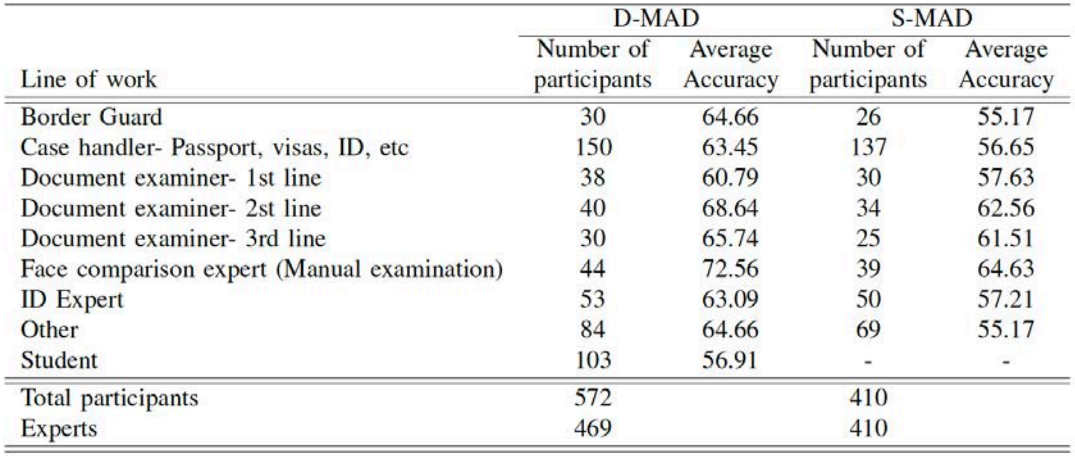
*Please remember to save your personal code **MJ7Se**.

[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: "Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?", https://arxiv.org/abs/2202.12426

Human Experts in MAD

Overall accuracy



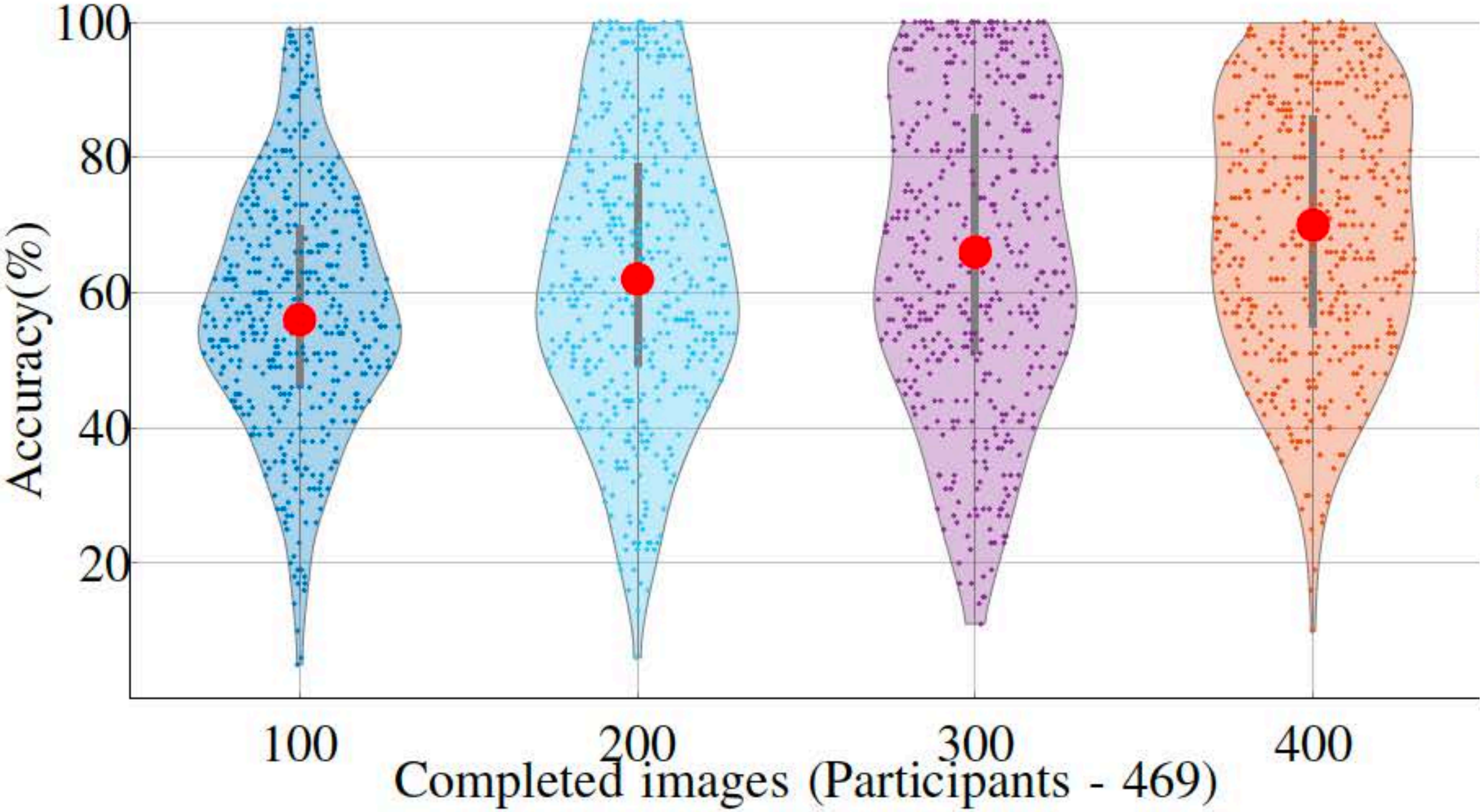


	D-MAD		S-MAD	
Line of work	Number of participants	Average Accuracy	Number of participants	Average Accuracy
Border Guard	30	64.66	26	55.17
Case handler- Passport, visas, ID, etc	150	63.45	137	56.65
Document examiner- 1st line	38	60.79	30	57.63
Document examiner- 2st line	40	68.64	34	62.56
Document examiner- 3rd line	30	65.74	25	61.51
Face comparison expert (Manual examination)	44	72.56	39	64.63
ID Expert	53	63.09	50	57.21
Other	84	64.66	69	55.17
Student	103	56.91	-	-
Total participants	572		410	
Experts	469		410	

[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: “Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?”, https://arxiv.org/abs/2202.12426

Human Experts in MAD

Does exposure to morphed images help?



(a) D-MAD Accuracy

[GOD2022] S. Godage, F. Løvåsdal, S. Venkatesh, K. Raja, R. Raghavendra, C. Busch: “Analyzing Human Observer Ability in Morphing Attack Detection - Where Do We Stand?”, https://arxiv.org/abs/2202.12426

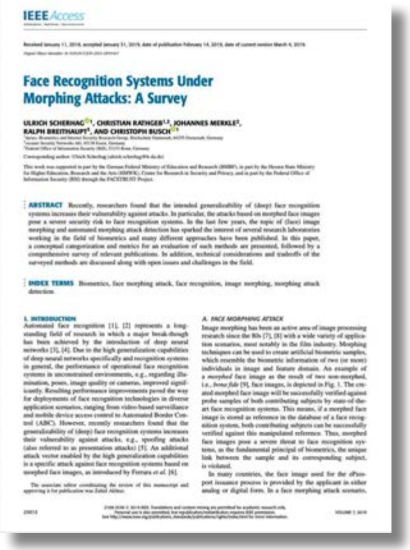
More information

The MAD website

https://www.christoph-busch.de/projects-mad.html

The MAD survey papers

- U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch: "Fa Systems under Morphing Attacks: A Survey“, in IEEE Access, (2019) https://ieeexplore.ieee.org/document/8642312


IEEE Access

Face Recognition Systems Under Morphing Attacks: A Survey

ULRICH SCHERHAG[1], CHRISTIAN RATHGEB[1,2], JOHANNES MERKLE[3], RALPH BREITHAUPT[3], AND CHRISTOPH BUSCH[1]

- S. Venkatesh, R. Raghavendra, K. Raja, C. Busch: "Face Morphing Attack Generation & Detection: A Comprehensive Survey", in IEEE Transactions on Technology and Society (TTS), (2021) https://ieeexplore.ieee.org/document/9380153

Transactions on Technology and Society

Face Morphing Attack Generation & Detection: A Comprehensive Survey

Sushma Venkatesh Raghavendra Ramachandra Kiran Raja Christoph Busch
Norwegian University of Science and Technology (NTNU), Norway
E-mail: {sushma.venkatesh;raghavendra.ramachandra;kiran.raja;christoph.busch}@ntnu.no

More information on MAD

The 2021 NBL - EAB workshop

https://eab.org/events/program/229

- Luuk Spreeuwers (University of Twente) - recorded talk
  - Morphing Attacks on Face Recognition Systems
- David Robertson (University of Strathclyde) - recorded talk
  - Psychological Experiments on Morphed Faces
- Kiran Raja (NTNU) - recorded talk
  - Morphing Attack Detection Approaches
- Matteo Ferrara (University of Bologna) - recorded talk
  - Bologna Online Evaluation Platform
- Frøy Løvåsdal (Norwegian Police) - recorded talk
  - Morphing Attack Detection Capabilities of Human Examiners
- Mei Ngan (NIST) - recorded talk
  - Face Morphing Detection Evaluation
- Naser Damer (Fraunhofer IGD) - recorded talk
  - Generating Morphs with Generative Adversarial Networks
- Christian Rathgeb (Hochschule Darmstadt) - recorded talk
  - Detection of Face Beautification Manipulations
- Uwe Seidel (BKA)
  - Research Needs for Morphing Attack Detection

European Association for Biometrics eab Human Identity in Europe

References

Web

- ICAO: http://www.icao.int
- ICAO 9303: http://www.icao.int/publications/pages/publication.aspx?docnum=9303
- FRONTEX: http://frontex.europa.eu

Complementary reading

- Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States
- ISO/IEC 19794 Biometric data interchange formats
  - Part 4: Finger image data
  - Part 5: Face image data
- ISO/IEC 39794 - Extensible biometric data interchange formats
  - Part 4: Finger image data
  - Part 5: Face image data