Scope of 3rd Generation Passport Standards and relationship to ICAO

Christoph Busch
Convenor ISO/IEC JTC1 SC37 WG3

copy of slides available at:
https://christoph-busch.de/about-talks-slides.html
more information at:
https://christoph-busch.de/standards-sc37wg3.html
latest news at:
https://twitter.com/busch_christoph

EAB-RPC, September 15, 2020

NTNU

European Association for Biometrics
eab
Human Identity in Europe

ATHENE

da/sec
BIOMETRICS AND INTERNET-SECURITY RESEARCH GROUP

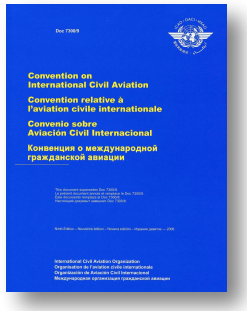
Overview

Structure of this session

- Christoph Busch
  - Scope of 3rd Generation Passport Standards and relationship to ICAO
- Olaf Henniger
  - The ISO/IEC 39794-1 Framework
- Greg Cannon
  - ISO/IEC 39794-4: Fingerprint image data
- Christian Croll
  - ISO/IEC 39794-5: Face image data
- Ralph Lessmann
  - Integration aspects

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
- 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

Standardised Travel Documents

History of the ICAO MRTD program

- Requirements for efficient civil aviation operations (Annex 9, Chicago Convention, 1944)
  - Art 13: regulations relating to entry, clearance, immigration, passports, customs
  - Art 22: prevent unnecessary delays
- MRTD Program
  - 1968: establishment of a Panel on Passport Cards
    - machine readable standardized passport book, initial issuance by Australia, Canada, USA
  - 1986: establishment of the TAG/MRTD (now TAG/TRIP)
    - comprised of government officials, expansion of scope to specifications for machine readable visa and cards

ICAO International Specifications

Why biometric data in travel documents?

- 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.*

Source: BSI

- Motivating factor #1:
  - Reduce transaction times (speed-up)

ICAO International Specifications

Motivating factor #2:

- More security!
- One individual - one passport

Principle of unique link

- 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/

ICAO International Specifications

Doc 9303 Structure: 12 parts (in the 7th edition)

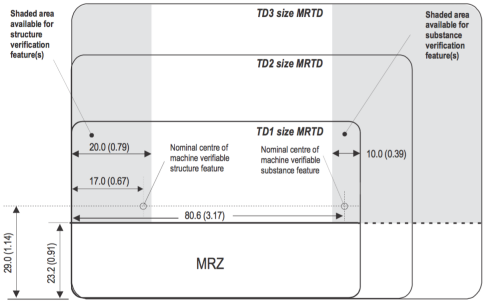
2015

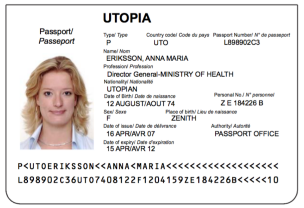
- Part 1 — Introduction
- Part 2 — Specifications for the Security of the Design, Manufacture and Issuance of MRTDs
- Part 3 — Specifications common to all MRTDs
- Part 4 — Specifications for Machine Readable Passports (MRPs) and other TD3 size MRTDs
- Part 5 — Specifications for TD1 size Machine Readable 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
- The 8th edition is expected to be endorsed by the TAG-TRIP in September 2020.
  - It will consist of 13 parts (P13: Visible Digital Seals)

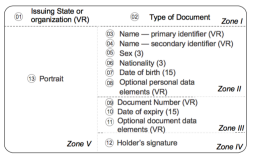
ICAO International Specifications

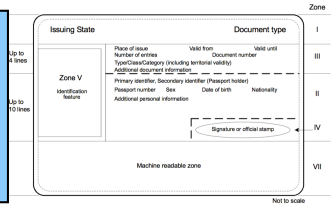
Doc 9303: relevant parts

Part 2: Specification for the Security of the Design	MRTD environment: design, production, issuance
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
Part 5:TD1 size MRTDs electronic citizen cards	sequence of data elements, truncation rules
Part 7: Machine Readable Visas (MRV)	specification which allow both visual and machine readable means
Part 10: Logical Data Structure (LDS)	specification for both visual and mach. readable







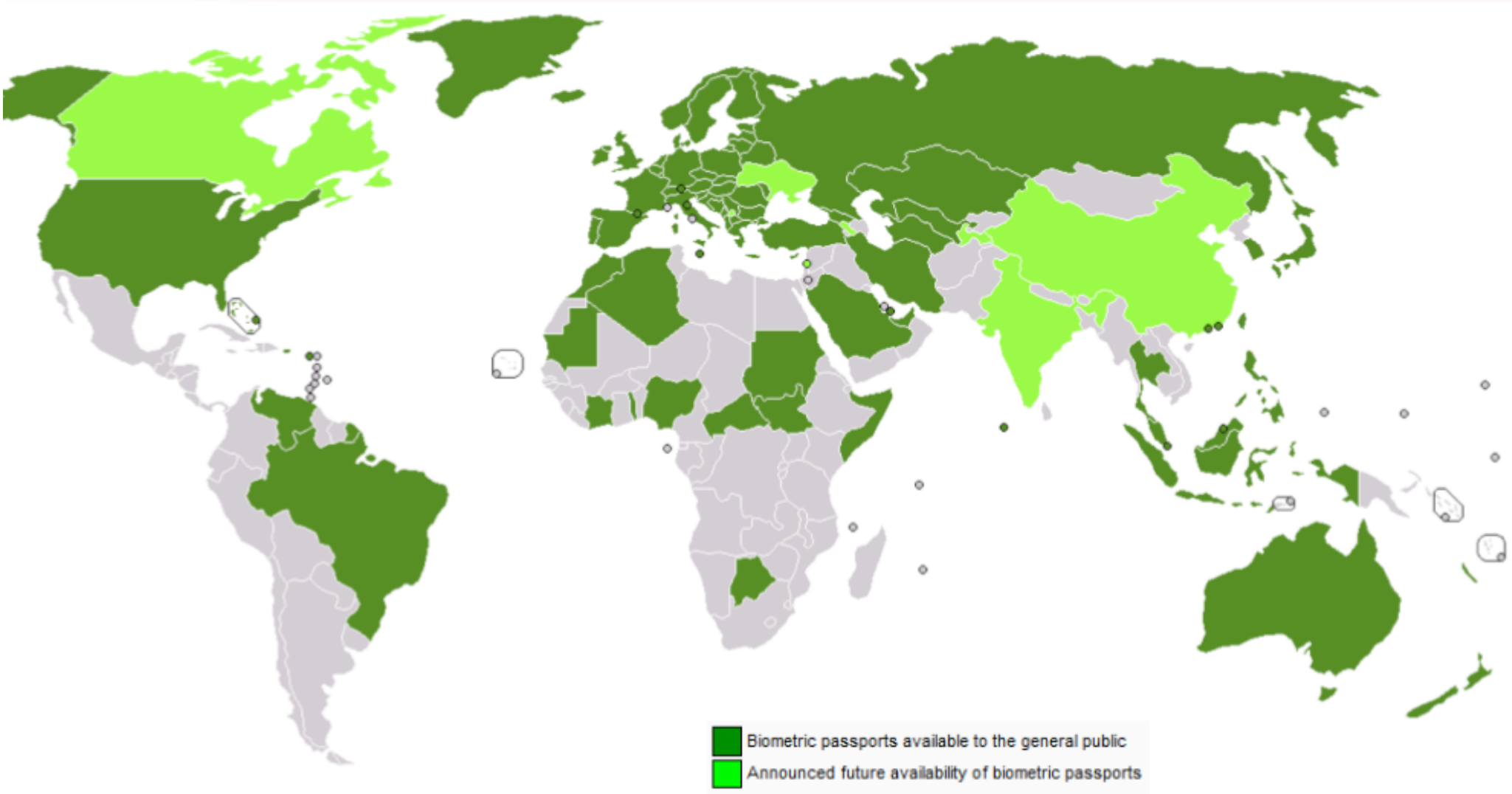


Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
	Additional Feature(s)	DG3	Encoded Finger(s)
		DG4	Encoded Eye(s)

Deployment of Biometric Passports

700+ million ePassports

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



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

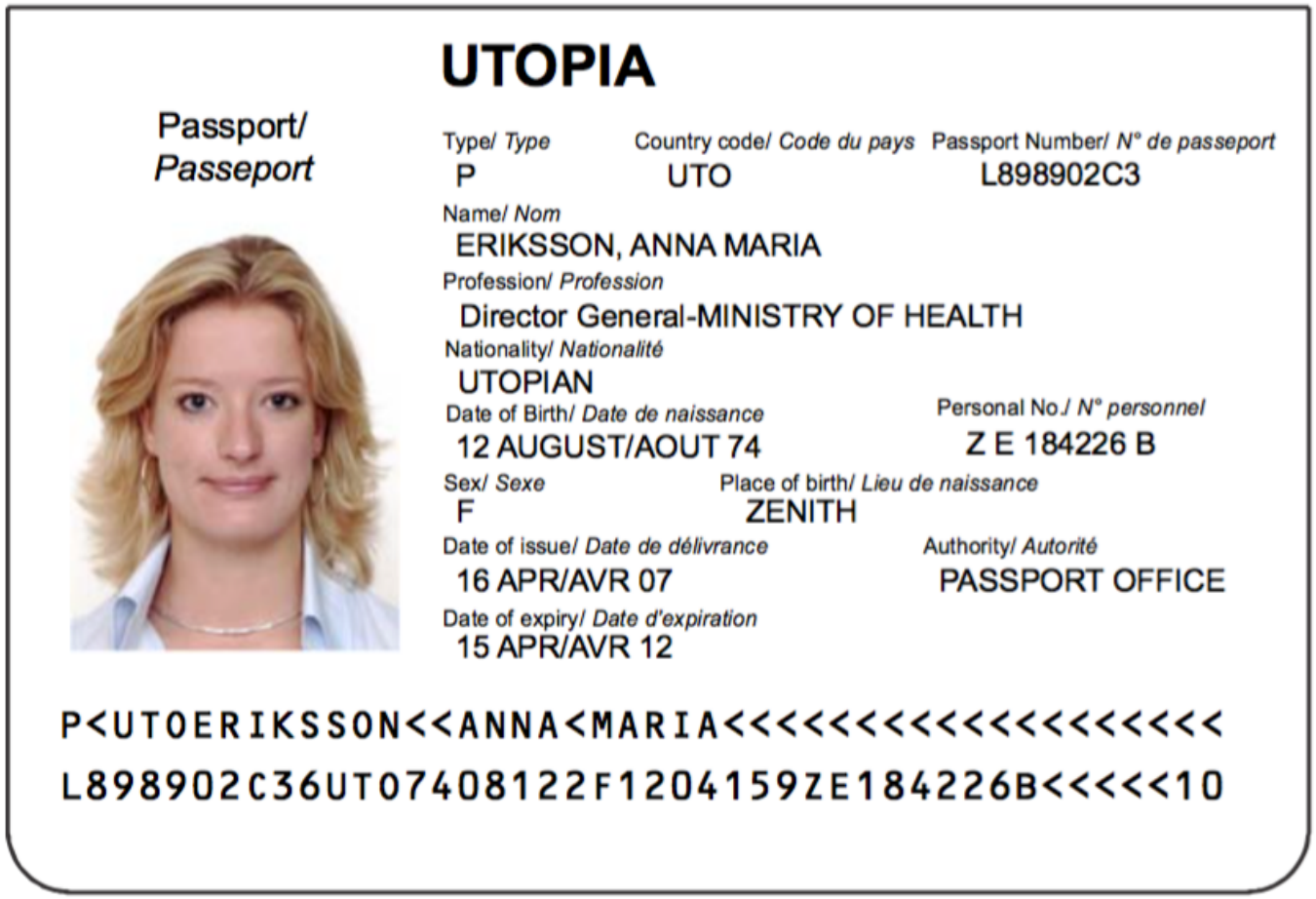
- Reason for and objectives
  - *"The inclusion of biometric identifiers, and particularly the inclusion of fingerprints, renders documents more reliable and secure. In that context, it is of crucial importance to phase out documents with weak security features as quickly as possible."*
  - *"The inclusion 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

ePassport - Data Page

Elements

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



Source: ICAO 9303 Part 4, 2015

ePassport Data Group Details

Data stored on the chip (LDS)

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

- DG3: Fingerprint image of left and right index finger

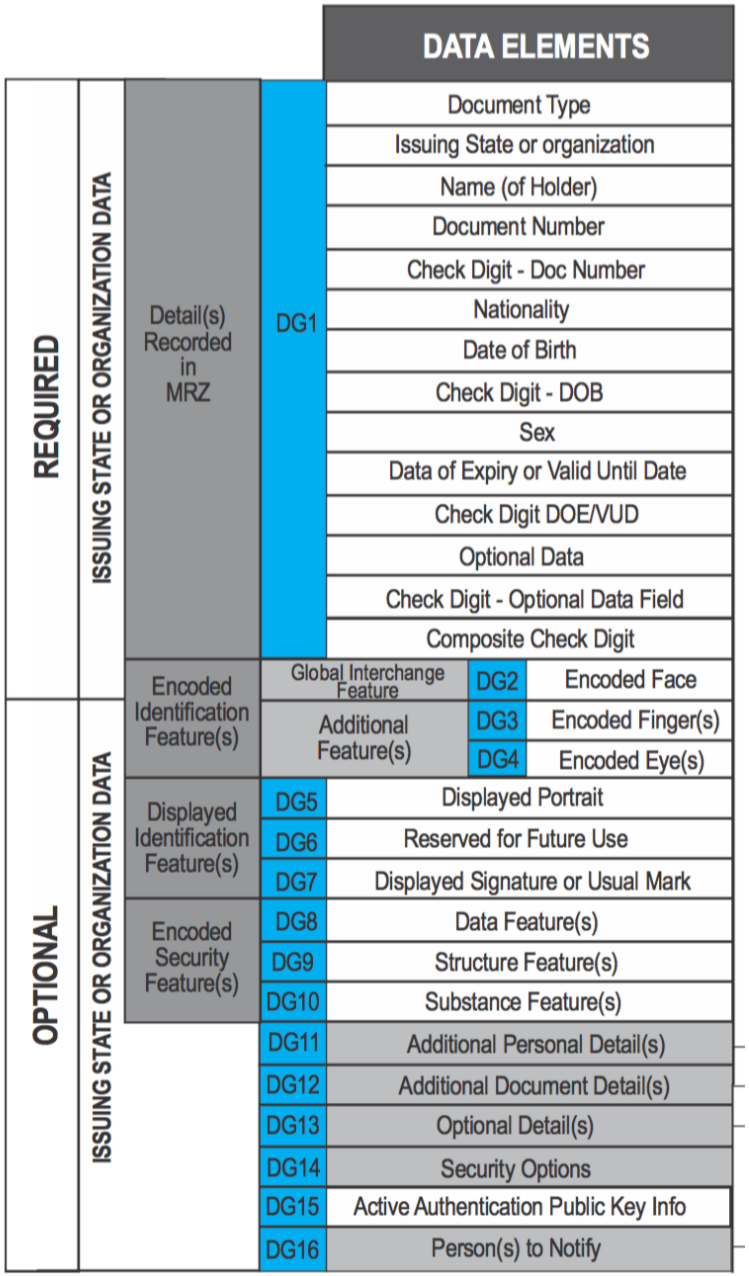
- DG4: Iris image (not in the EU)

....

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

Document Security Object

- Hash values of DGs



Source: ICAO 9303 Part 10, 2015

ePassport Details

Data to be stored in the RFID-Chip

Oct 2005

- 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)

- 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

New in 2020

Scope of 39794

Scope

ISO/IEC JTC1 SC37 WG3

Terms of Reference of the Working Group:

- To consider the standardisation of the content, meaning, and representation of biometric data formats which are specific to a particular biometric technology. To ensure a common look and feel for Biometric Data Structure standards, with notation and transfer formats that provide platform independence and separation of transfer syntax from content definition

“Getting equipment to understand each other”

Objectives and Design Criteria for 39794

Agreed between ICAO/SC17WG3 and SC37WG3

Jan 2014

- The encoding of G3 should be FORWARD compatible, such that G3 readers can parse G3+ passports with extended data structure as long as the respective G3+ data structure contains at least the image data in the format that was defined in G3.
  - Thus anticipate future new fields.
- The encoding of G3 should allow a trans-codable TLV-BIN record, that is at most marginally larger than a G1 binary record
- The design of the G3 should minimize the increase of the read-out time for a passport reader.
- G3 encoded records (XML or TLV) must be trans-codable within the Generation

FORWARD compatibility in 39794

Defined between ICAO/SC17WG3 and SC37WG3

- "A parser must also be able to read data records, which are based on newer standards as the parser itself, and understand data items which existed in older or equal standards of the parser.
  - All newer data item shall not disturb the parsing process and shall be ignored.
  - Newer standards must at least include the mandatory data items of the previous standards."

Jan 2014

- Example 1:
  - A G1 e-passport reader is not able to read a G2 record. Hence, it is not forward compatible.
- Example 2:
  - In order to be forward compatible, a G3 e-passport reader would need to be able to read the G3 features that are maintained in records of later generations

Adoption of ISO/IEC 39794 by ICAO

ICAO TAG/TRIP to confirm the 8th edition of Doc 9303

- Later in 2020 ICAO Technical Advisory Group on Traveller Identification Programme (TAG/TRIP) will confirm the 8th Edition of Doc 9303.

Fall 2020

- Doc 9303 contains in its Part 9 on Deployment of Biometric Identification and Electronic Storage of Data in MRTDs the timeline for the transition from ISO/IEC 19794-X 1st Edition to ISO/IEC 39794-X as follows:
  - ISO/IEC 39794 succeeded ISO/IEC 19794:2005

Source: Tom Kinneging - Convenor ISO/IEC JTC1 SC17 WG3

Transition Time Line from 19794 to 39794

The following transition time table has been defined:

- Passport reader equipment MUST be able to handle ISO/IEC 39794 data by 2025-01-01 after a five years preparation period starting 2020-01-01
- Between 2025 and 2030, passport issuers can use the data formats specified in ISO/IEC 19794-X:2005 or in ISO/IEC 39794-X during a five years transition period.
  - During this transition period, interoperability and conformity testing will be essential.
- From 2030-01-01 on, passport issuers MUST use ISO/IEC 39794-X for encoding biometric data.

Source: Tom Kinneging - Convenor ISO/IEC JTC1 SC17 WG3

Summary

The evolution took some time …

- … but the result is ready to walk and work

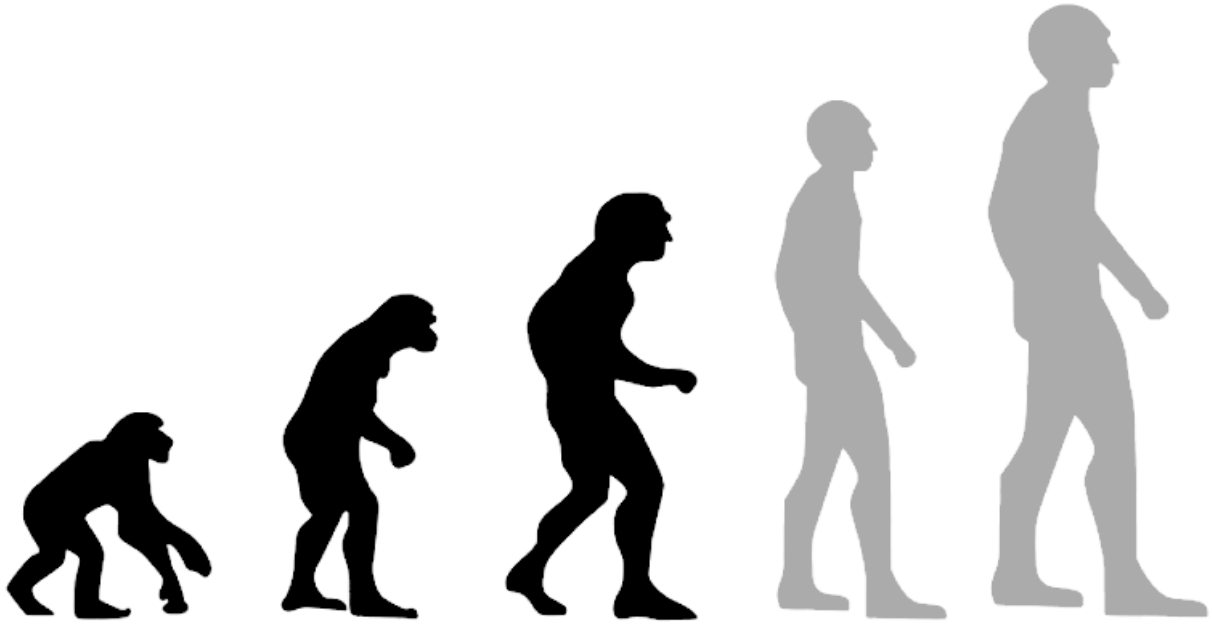
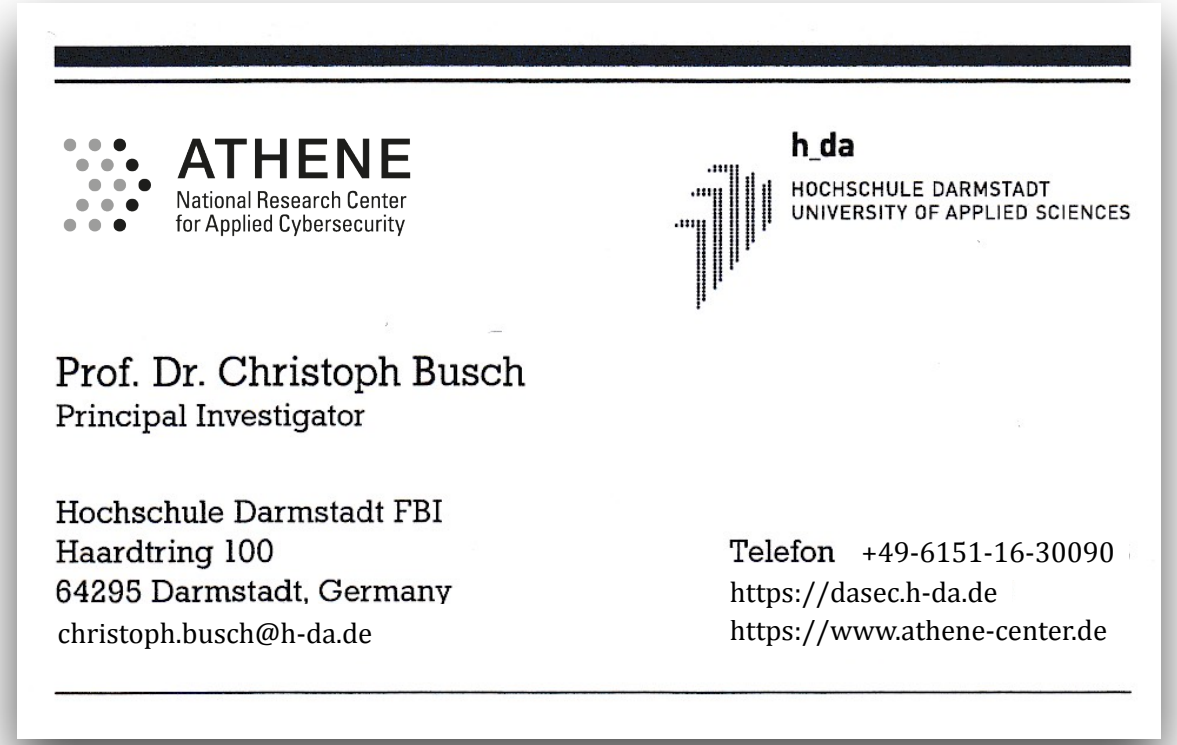


Image Source: https://pixabay.com/de/illustrations/evolution-entwicklung-zukunft-3543775/

Contact


ATHENE
National Research Center
for Applied Cybersecurity
h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
Prof. Dr. Christoph Busch
Principal Investigator
Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@h-da.de
Telefon +49-6151-16-30090
https://dasec.h-da.de
https://www.athene-center.de