



| ICAO

2026 ICAO **TRIP** SYMPOSIUM

22 - 24 SEPTEMBER | MONTRÉAL, CANADA



00 1 10 100 1000 1 10 100 10
00 1 10 100 1000 1 10 100

Dion Chamberlain

General Manager – Engagement, Data and
Innovation & Chief Advisor Traveller Identification

Department of Internal Affairs, Aotearoa New
Zealand

Chairperson – ICAO Implementation and Capacity
Building Working Group (ICBWG)

ePassport History

9/11 changed the civil aviation world

- Security architecture of ecosystem
- Protect people and critical infrastructure



- Traveller identity and travel documents recognised as a critical component
- Accelerated ePassport adoption and ongoing development
- In response to US-Visa-Waiver Programme changes
 - Australia, New Zealand and Belgium implemented first compliant ePassports

ICAO TRIP 2026

-
- AOTEAROA / NEW ZEALAND
- PASSPORT
- Māori / Type: Whakamua / Country: Rauwharua / Passport No. RA000001
- English / Name: WHAKAAHUA
- English / Given name: AROHA MARY RAUMATI
- Issued Authority: NEW ZEALAND
- Date of Birth: 01 NOV 1988 F
- Place of Birth: TAIHAPE
- Date of Issue: 01 JAN 2020
- Date of Expiry: 01 JAN 2030
- Issued Authority: DIA WLG



Digital Uplift Brought Opportunity



Verifiable source information makes it easier to determine who you **DON'T** care about – which is the biggest benefit



Facilitating **99%** low risk by increasing automation and **focus resource on finding the less than 1% bad actors**



- Manage risk at point of embarkation and arrival
- Streamline biometrics use
- Linked intelligence and watchlists
- Increased automation, analytics and data

Passport Issuing Authorities

Facilitation mindset for issuance

- Customer, convenience, efficiency focus
- Online and digitally enabled applications
- Automated decision making
- Routine use of biometrics
- Verifying source information
- Increased data analytics

Risk-based decision making in the issuance process

- Behaviours and indicators within the system
- Increased ability to **NOT** treat everyone at the same risk level – more nuanced approach, combined information



Evidence of Identity (EOI)

Foundational thinking

- EOI based on gaining confidence
- NO absolutes – context specific
- New EOI Guide about to be published
 - Traffic light – what characterises different zones?
 - Finding other evidence to ‘Go to Green’

RED ZONE

Non-verifiable information and insecure documents

LOW CONFIDENCE

AMBER ZONE

Reliance on secure but unverifiable documents

Non-centralized information

Limited or no biometric matching

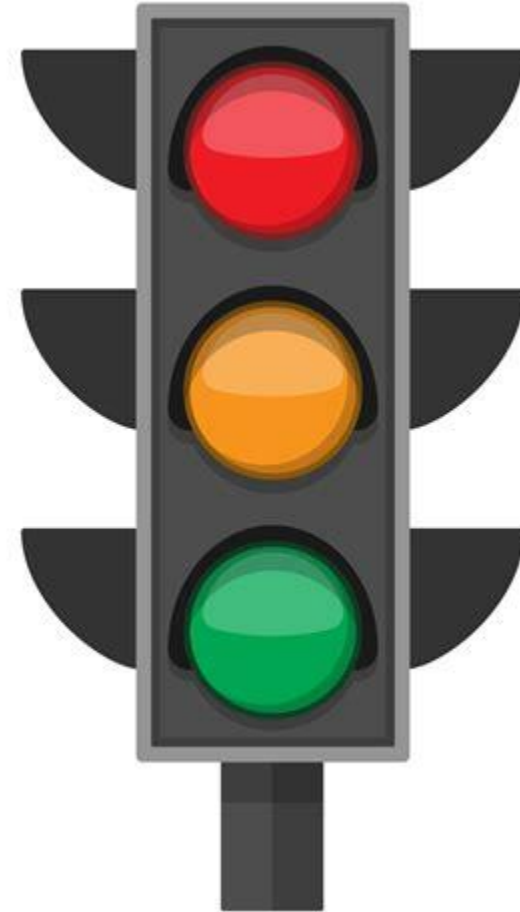
MEDIUM CONFIDENCE

GREEN ZONE

Verifiable foundational documents

Biometric matching

HIGH CONFIDENCE

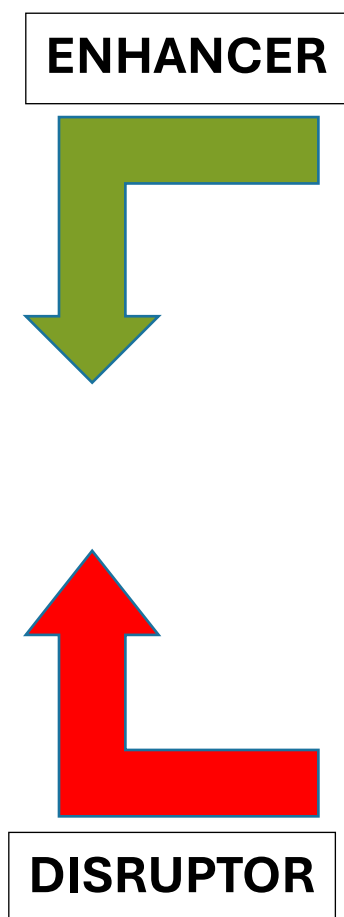


So in a world where expectation is shifting to digital credentials for passports and border clearance, how do we adjust our EOI?

The Digital World

- Increasingly harder to trust documents on face value – significant investment required to secure documents throughout the entire identity chain
- ePassports, verifiable digital barcodes, biometric matching
 - Verifiable data to augment the physical
 - Automate to increase efficiency and reduce human factors
 - Machines are more accurate and consistent
- BUT ... there are disruptors to the technologies – **GREEN** is not a forever state – EOI re-evaluation is constant, just like threats

Evidence of Identity (EOI)



RED ZONE

Non-verifiable information and insecure documents

LOW CONFIDENCE

AMBER ZONE

Reliance on secure but unverifiable documents

Non-centralized information

Limited or no biometric matching

MEDIUM CONFIDENCE

GREEN ZONE

Verifiable foundational documents

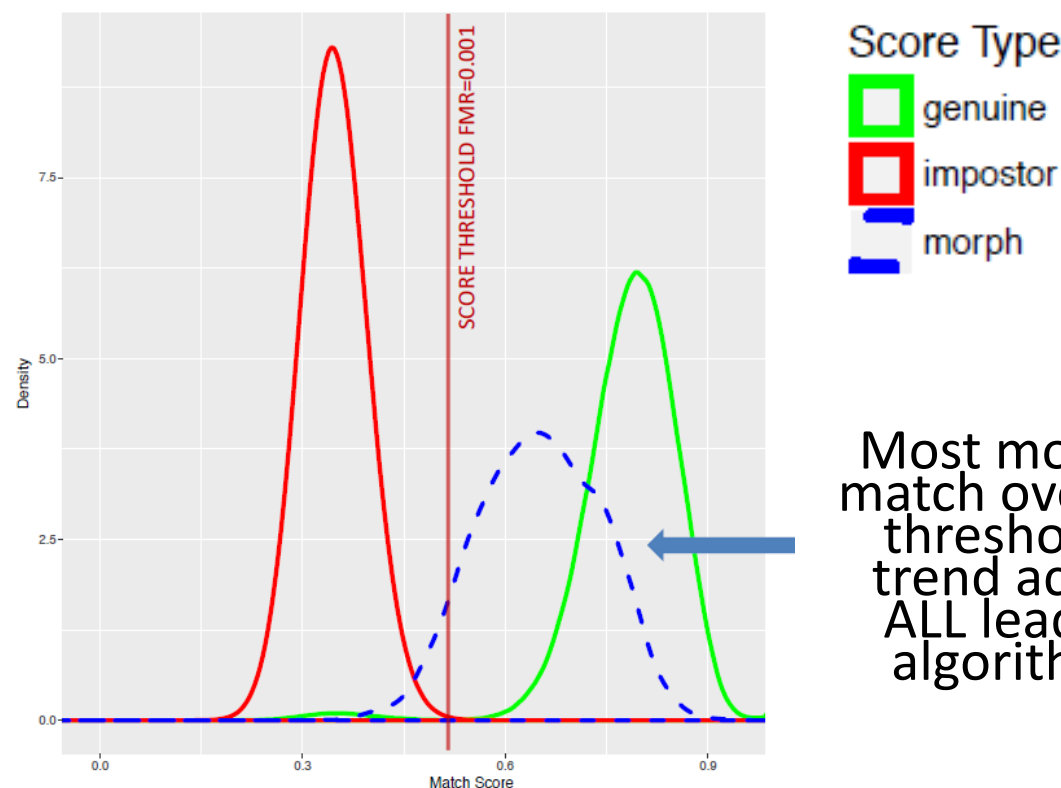
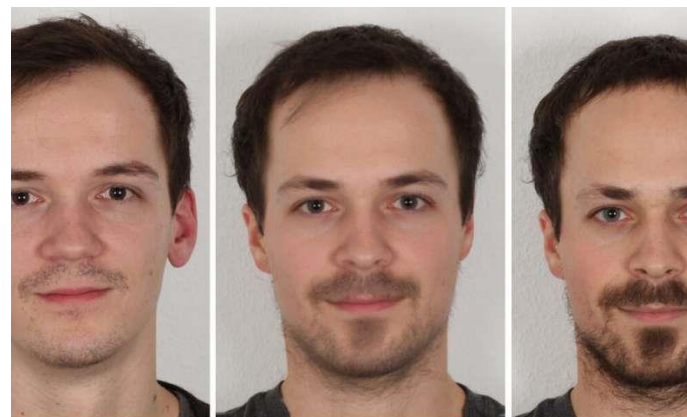
Biometric matching

HIGH CONFIDENCE

Digital Threats

- Digital is fast moving
 - Artificial Intelligence (AI)
 - Standards fragmentation
 - Ecosystem complexity
- **AND**

PHOTO MORPHING



Most morphs
match over the
threshold –
trend across
ALL leading
algorithms

NIST - “Morphing is Easy”

Morphs ... response

There was a time when we were super worried about tombstone fraud ...

But if someone suggested removing all the tombstones ...



And this is **also** my face when someone suggests the only way to solve morphing is to make every single applicant appear in person for live photo capture.

Service
Excellence



Risk



Morphs ... and everything else

One threat vector among many - maybe not having a centralised biometric identity database is a bigger risk?

Morphs are:

- Still part of an operational context – with controls
- Still needs an available identity – through collusion or theft.
- Found sometimes through data/risk indicators
 - Multiple 1:Many high score biometric matches within your own system an indicator
 - Applicant risk behaviours
 - Morph detection software? Digital footprint? Differentials?

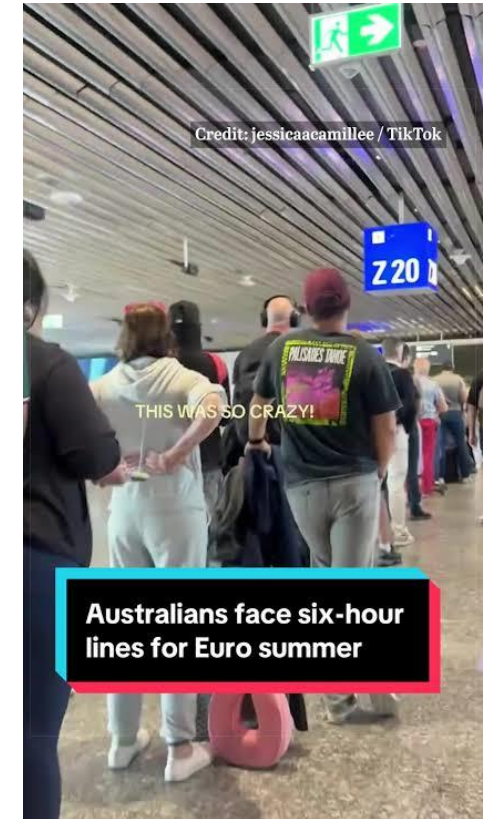
Morphs ... and everything else (2)

Strategy for morphing and anti-fraud in the digital world more generally:

- DEFENCE IN DEPTH / AGILITY / CHANGE
- Securing the online channel – replicating in-person aspects (a live human) and taking a snap of a secure video feed for the passport rather than allowing the applicant to upload their own photo
- Validating data, proactive contact, consistency over time, other sources/information, social footprint
- Understanding threat vectors - we have to know where the digital world might fail us so we can respond

The role of the physical world ...

- We can't go back ... digital and automation is a foundational enabling technology
- Need to understand when to intervene, when the physical controls and security play a part and how
- In person and physical processes can be done by exception ... **BASED ON RISK**

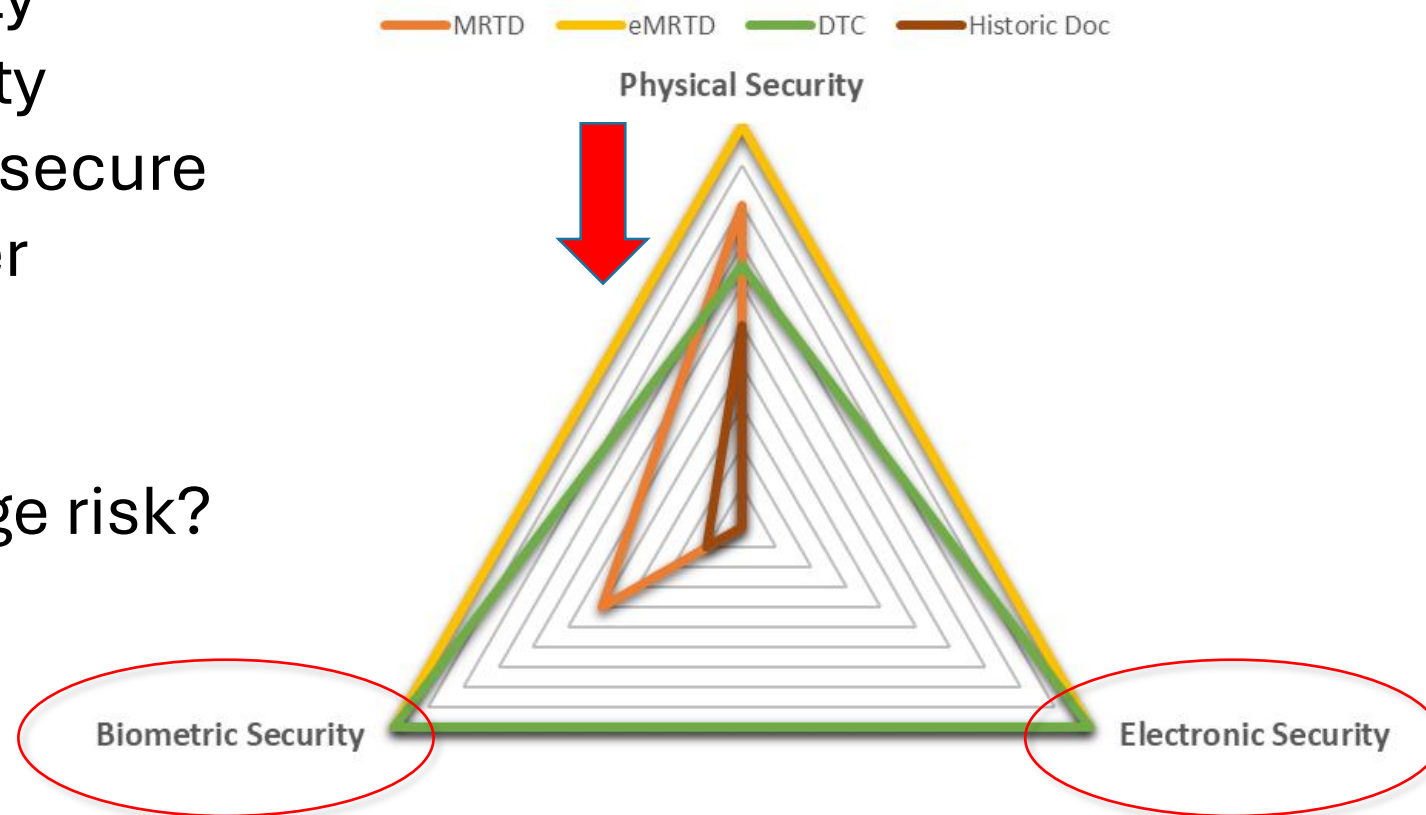


The Physical Security Gap - DTC

Without the passport or officially signed DTC-PC, physical security dynamic changes – it is **NOT** as secure as a current eMRTD unless other things change or augment

Does other uplift cover or change risk?

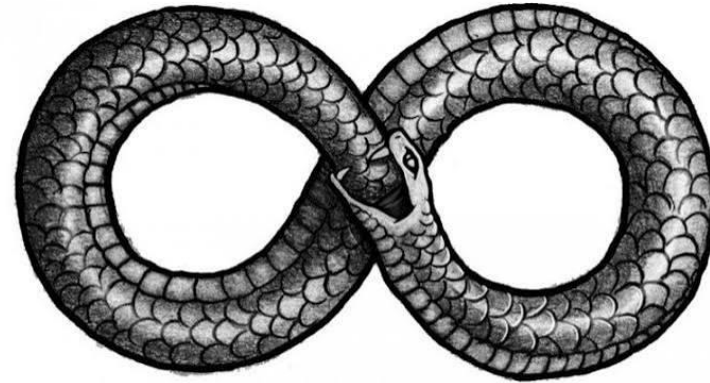
- Wallet and device security
- Secure transmission
- Broader airport, border and aviation security architecture
- **Integrated border/other data**



*Diagram from Dr. Uwe Seidel – Chair ICAO NTWG

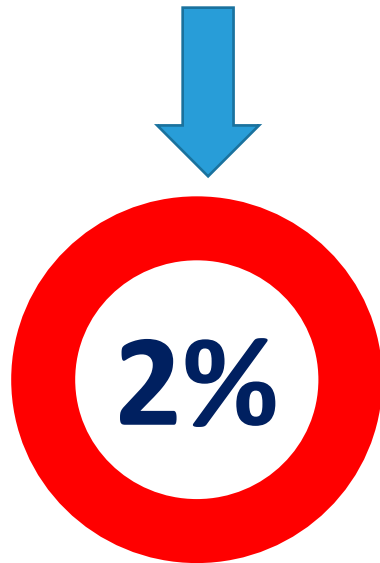
Digital Threats ... are real

- AI – ability to generate images, attack and hack data, research and create identities
- Arms race to stay ahead and keep the digital world secure ... like a snake eating its own tail



- Post Quantum Computing and threats to cryptography

ICBWG Linked 



Thank You

