Evidence of Identity: A Case Study on Risk and Automation

Dion Chamberlain

Manager Product Development, Identity and Life Events Department of Internal Affairs, New Zealand

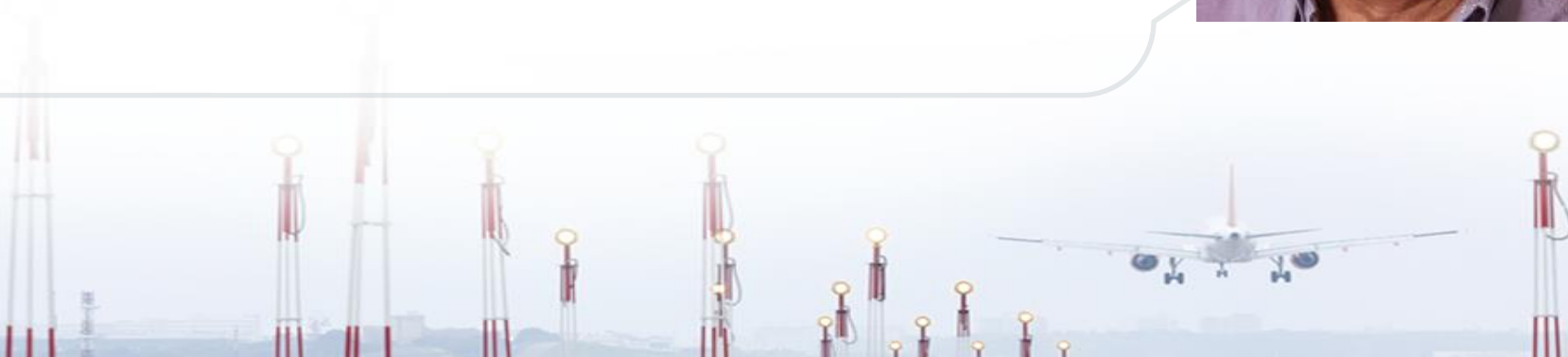*Secretary – ICAO Implementation and Capacity Building Working Group (ICBWG)*

5-7 June, Brasilia 2018

What Mr Dharwadker said …

- Identity is **diverse, dynamic and complex**

- There is **no "silver bullet"** and **no "one-size-fits-all"**

- **Combination** of information to minimize risk

EOI Authentication Principles

Principle 1 - Identity Exists

> **Objective A - The identity exists (i.e. is not fictitious)**

> **Objective B - The identity is living**

Principle 2 - Applicant links to Identity

> **Objective C - The presenting person links to the identity**

> **Objective D - The identity is UNIQUE to your system (i.e. only has one claimant)**

Principle 3 - Applicant uses Identity

> **Objective E - To provide confidence of the presenter's use of the identity in the community**

ICAO Guide on EOI: Example Assessment Table

Table 2:

		Foundational Document	Checks and Measures				Number of checks available
Principle 3: Presenter uses Identity	C - Applicant links to the identity	1: Assertion by a referee	Known by Authority	Matches your database?	Referee trusted by your authority	Matches a trusted group of people	
		2: In-person verification	Self-Supplied Photo ID?	Trusted photo-ID authorities	Are they in the authority's records?	Staff trained in document comparison	
		3: Biometric recognition	Applicant photo database	Other biometrics databases	External authority databases	Historic biometric information	
		4: Interview	Staff trained to conduct interview	Information on applicant sufficient	Enough capacity and infrastructure	Policy on acceptance of evidence	
	D – Sole claimant to unique identity	5: Check authority records	All applications recorded	Staff trained in identifying records	Systems for data matching	Historic records available	
		6: Biometric recognition	Photographs of all applicants	Availability of historic biometrics	Biometric comparisons	Other biometrics stored	
		Additional Evidence					

- Evaluation: follow EOI principles to systematically document and understand your **'identity ecosystem'** and key risks

- Analyse ALL potential document, record or information sources available and its value in an EOI process (a matrix is helpful)

- Understand the security of "foundational" records, data and the issuance process that sits behind them

- Identify gaps and look to other areas of EOI to increase confidence ... **THEN design** the approach.

High Degree of Identity Confidence Required
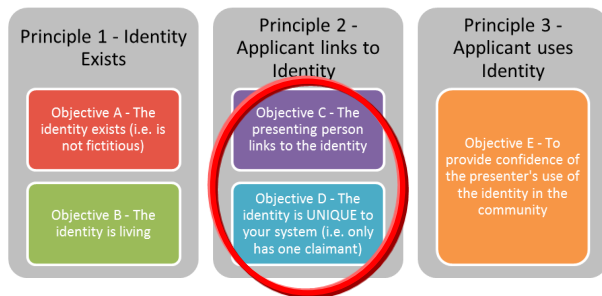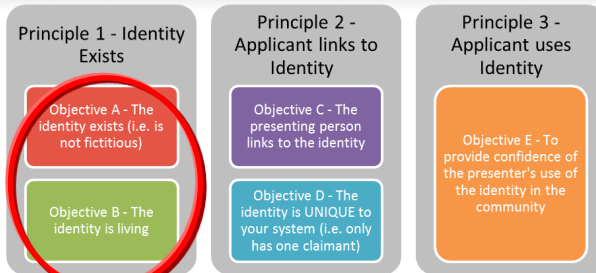
So what? Why invest in foundational EOI?

- We all face cost pressures – demand for efficiency gains
- High confidence in EOI and resulting data assets and systems **enables** efficiencies, costs savings and new services
- Robust first-time interaction for travel documents means **subsequent contact can leverage** off initial EOI
- A well-understood EOI approach will enable **more effective targeting of resources** (people and system design)

Risk

Service
Excellence

Case Study: New Zealand

- Shift to 5-year validity in 2005
- Sharp volume increase in 2010/11 (almost double)
- Needed to increase production without increasing staff

Approach needed to be a holistic:

- Productivity and efficiency gains
- Increase integrity of data and process
- **Leverage our existing knowledge and investment - technology and quality EOI data**

Leverage EOI: Identity Exists

- Re-use the passport data for renewals
- Remove waste steps – why recheck documents?
- Death checks against central database
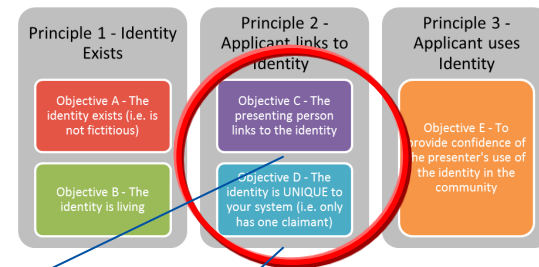- Automated checking – faster and more accurate

Principle 1 - Identity Exists
- Objective A - The identity exists (i.e. is not fictitious)
- Objective B - The identity is living

Principle 2 - Applicant links to Identity
- Objective C - The presenting person links to the identity
- Objective D - The identity is UNIQUE to your system (i.e. only has one claimant)

Principle 3 - Applicant uses Identity
- Objective E - To provide confidence of the presenter's use of the identity in the community

Applicant Links and is UNIQUE to the System: What is possible if you have high confidence in uniqueness to the database?
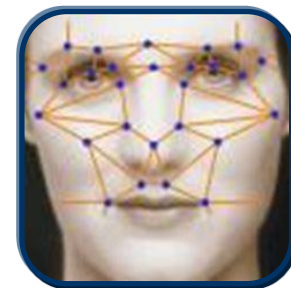
Confidence in UNIQUENESS: **Biometrics**

- In order to ensure we could use FR effectively, significant time and resource was invested in cleaning up our database
- Many to Many match:
  - 4.5 Million images, 21 Trillion matches, 210,000 matches of interest
  - Remove poor quality images
  - Merge or 'tag' duplicate records
  - Identify fraudulent activity and modify risk profiles

New Approach to Biometrics:

- The best use of biometrics from a business perspective is to facilitate automation and increased productivity (1:1 match for renewals, 1:N for new applications)
- Security benefits are a welcome bonus ...

Principle 1 - Identity Exists
- Objective A - The identity exists (i.e. is not fictitious)
- Objective B - The identity is living

Principle 2 - Applicant links to Identity
- Objective C - The presenting person links to the identity
- Objective D - The identity is UNIQUE to your system (i.e. only has one claimant)

Principle 3 - Applicant uses Identity
- Objective E - To provide confidence of the presenter's use of the identity in the community

Leverage Data: Social Footprint

- Identity Referee
- Known to our database and contactable
- Continuity and longevity of information
- Starting to use address verified

Overlay Automated Risk Profile

- Intelligence
- Risk indicators
- Adjusted tolerances for facial recognition

| Principle 1 - Identity Exists	Principle 2 - Applicant links to Identity	Principle 3 - Applicant uses Identity
Objective A - The identity exists (i.e. is not fictitious)	Objective C - The presenting person links to the identity	Objective E - To provide confidence of the presenter's use of the identity in the community
Objective B - The identity is living	Objective D - The identity is UNIQUE to your system (i.e. only has one claimant)	

The Outcome

- 128 automated checks – double passport volume without staff increase
- Staff are concentrating their time on exceptions and NOT reviewing every single piece of information received
- Data accuracy (reduction in forms)
- Renewal services entirely online – started with renewals and built (children, family groups, urgents, lost/stolen)
- Over 50% of online pass all assessments and require NO entitlement decision from a passport officer
- Costs savings and improved customer satisfaction
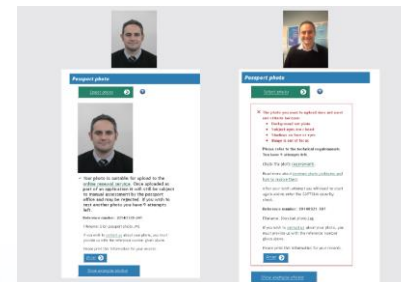
Top Takeaways

- Identity verification is not absolute – it is dynamic, based on context, probabilities and levels of confidence

- REVISIT your approach to EOI, systems and processes - develop a case for investment in EOI based on security **AND efficiency**

- Develop and maximise your critical EOI data assets – robust first up processes allow automation and more informed risk-based EOI decisions

- Look for a flip-side benefit to your – if there is an EOI technology you are using to guard against something, there is a good chance it will facilitate something too
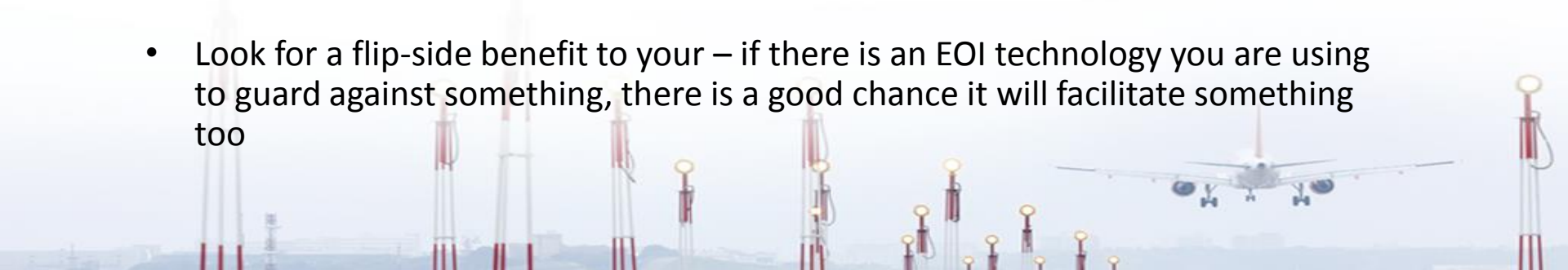
ICAO

North American Central American and Caribbean (NACC) Office
Mexico City

South American (SAM) Office
Lima

ICAO Headquarters Montréal

Western and Central African (WACAF) Office
Dakar

European and North Atlantic (EUR/NAT) Office
Paris

Middle East (MID) Office
Cairo

Eastern and Southern African (ESAF) Office
Nairobi

Asia and Pacific (APAC) Sub-office
Beijing

Asia and Pacific (APAC) Office
Bangkok

dion.chamberlain@dia.govt.nz

icbwg@icao.int

@ICBWG

THANK YOU