



| ICAO

2026 ICAO **TRIP** SYMPOSIUM

22 - 24 SEPTEMBER | MONTRÉAL, CANADA

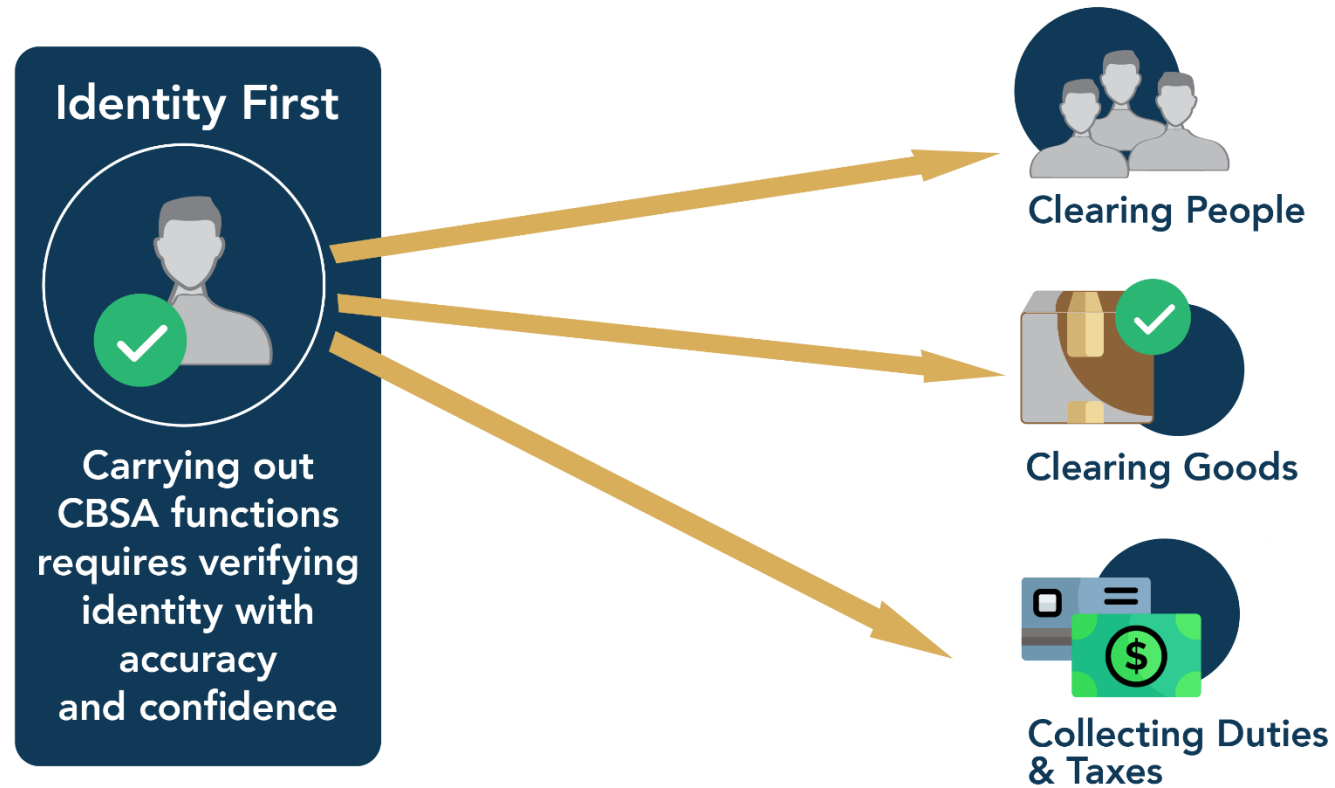


00 1 10 100 1000 1 10 100 10
00 1 10 100 1000 1 10 100

Justin Ikura

Director, Identity Management Division
Canada Border Services Agency (CBSA)

Verifying Identity is at the core of delivering our Mandate



What Are Borders Concerned About?



Are you the rightful bearer of the travel document being presented?



Do you present a risk to the country?



Are you entitled to enter the country?



Are you attempting to cross the border with anything of concern?

Page 10 of 10



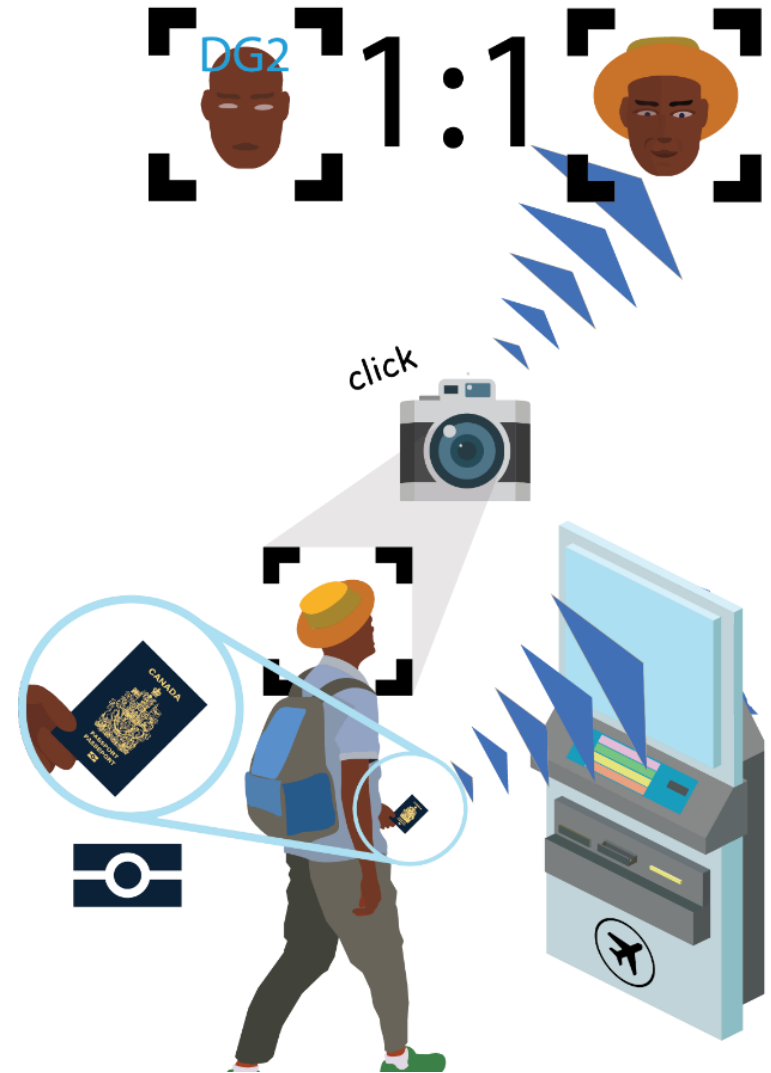
Biometrics can be used as a tool to support border management authorities in confirming that a traveller is the rightful bearer of the document being presented upon entry.



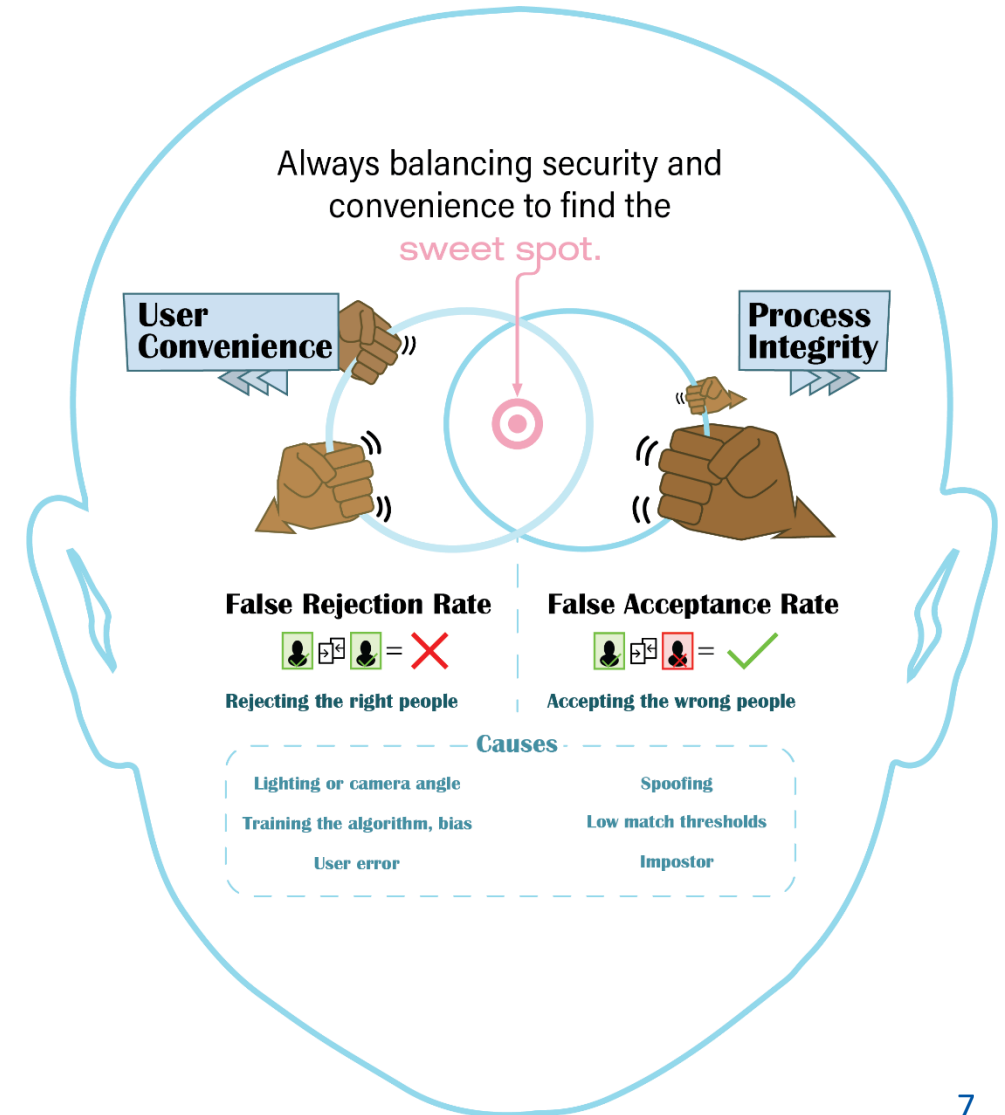
Biometrics are also often employed in pre-screening prior to travel to obtain a travel authorization.

Biometrics and Security

- Biometric matching technology is an effective tool for border management to balance security and facilitation at ports of entry.
- Affords opportunities to automate routine transactions.
- ePassports are a key enabling component of biometrics and border management, as they allow for real-time 1:1 verification
- Combined with other data, borders can significantly mitigate identity fraud at the border.
- Biometrics should be viewed as a tool in the border management toolbox.



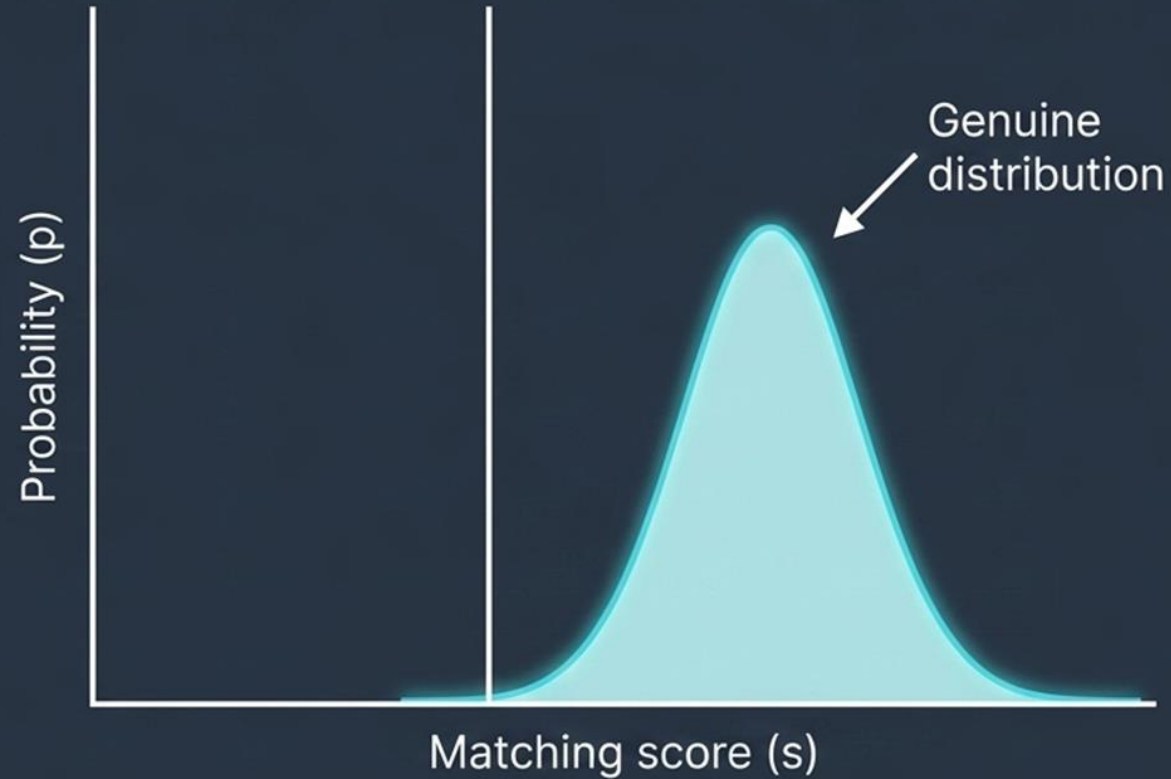
Balancing Objectives at the Border: Tuning to Meet Operational and Policy Needs



Legitimate travelers generate high matching scores

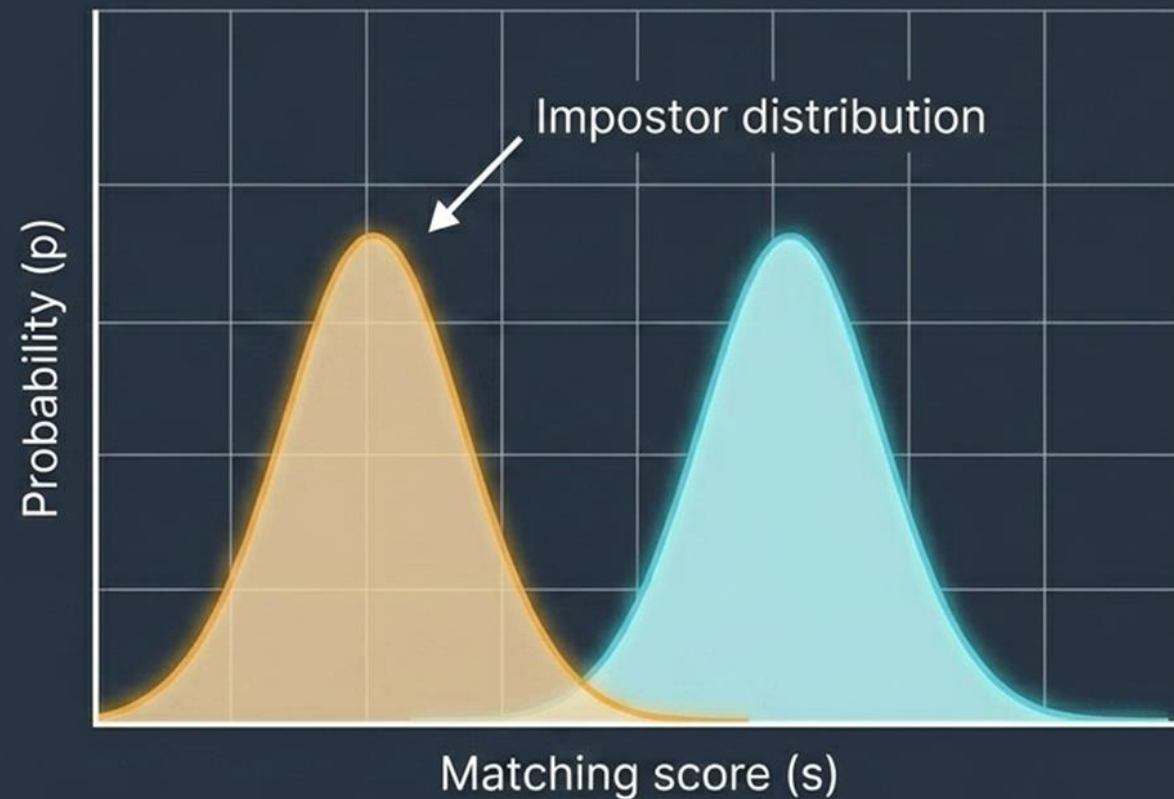
Every time a legitimate citizen uses an e-gate or kiosk, they generate a score.

Most of the time, the camera and algorithm perfectly match their face to their credential, resulting in a cluster of high scores on the right side of the spectrum.

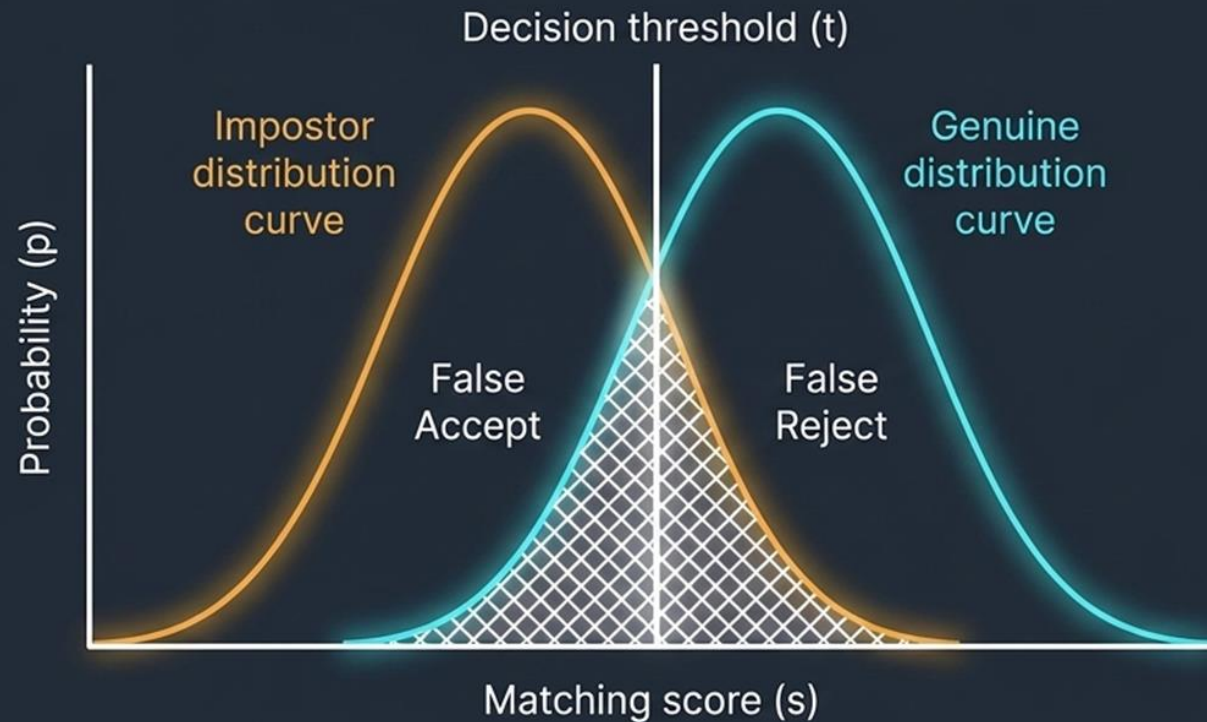


Bad actors and credential mismatches generate low matching scores

Conversely, when an impostor attempts to use someone else's credential, the system registers a low biological match, clustering these scores heavily to the left.



Environmental and biological friction forces these two populations to collide



Zone of Uncertainty

- Sensor degradation (smudged lenses, poor lighting)
- Biological changes (aging, weight loss, facial hair)
- Sophisticated spoofing attempts (masks, deepfakes)

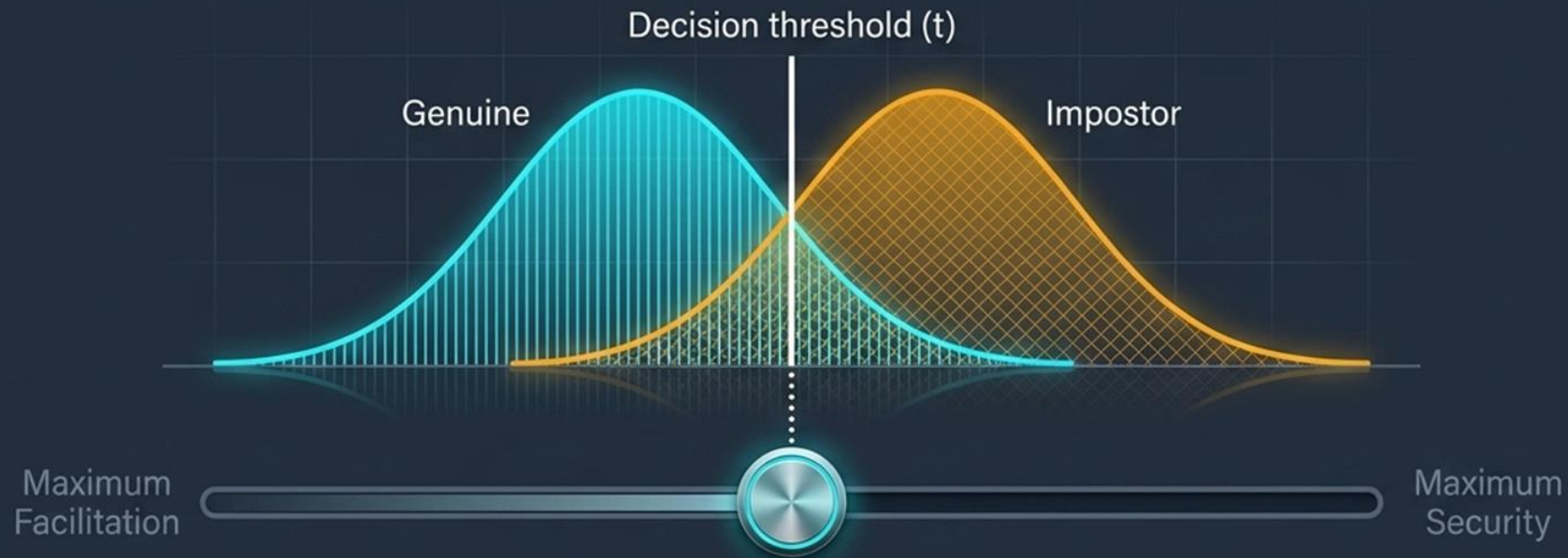
Inside the overlap, the algorithm can no longer mathematically guarantee identity

Is this a legitimate traveler with a bad passport photo?

Or is this an impostor wearing a high-quality disguise?

The algorithm has reached its **mathematical limit**.
The system requires a human directive.

Setting the threshold is a direct reflection of organizational risk appetite

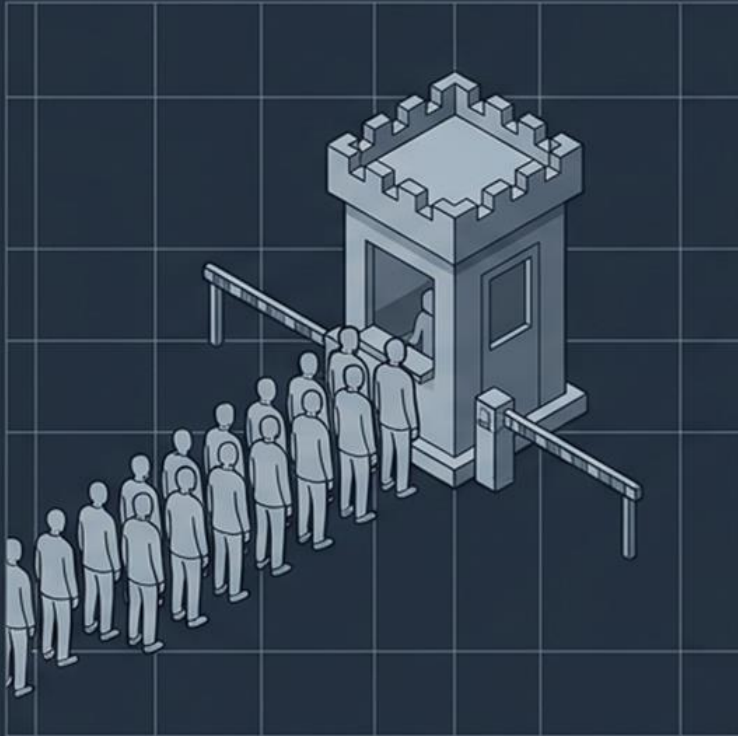


**Vendors supply the algorithms that shape the curves.
Only policymakers have the authority to move the line.**

Traditional Border Practices are Changing

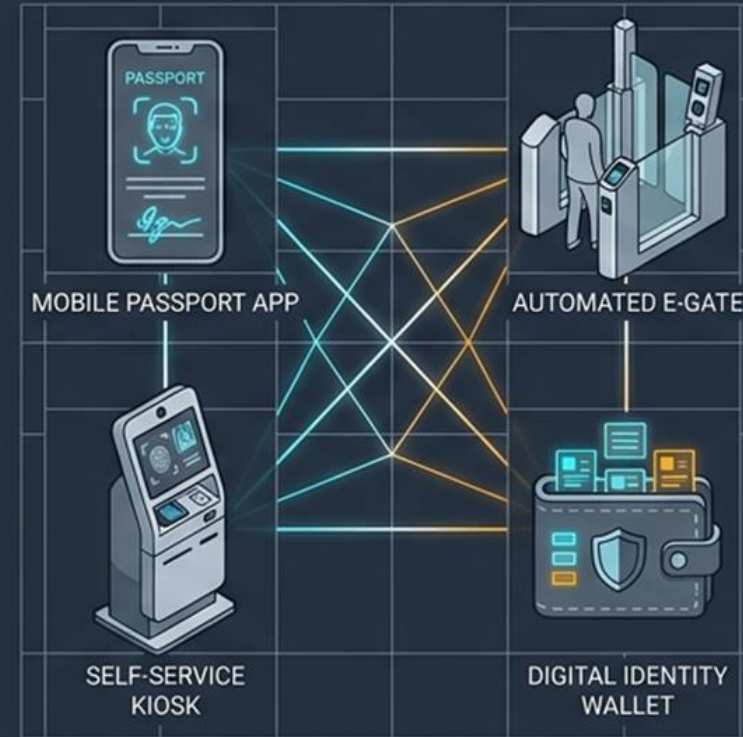
The physical border has dissolved into a distributed digital network

Past



Decisions are pushed outward.

Present



Every interaction is now a checkpoint.

Scale requires automation over human intuition.

Impact of New Technologies on Borders



Developments in digital credentials, mobile technology and biometrics are creating new opportunities to change the way we process travellers attempting to cross the border.

- Processing and interaction can begin earlier in the process of travel, including at the time of pre-screening.
- Value-generation relies on intergovernmental/stakeholder cooperation – identity transactions should be synched.



Deploying these new technologies earlier and throughout the continuum does create new risks that need to be accounted for and mitigated (i.e., presentation attacks, injection attacks and facilitation over security).



Border Processing of the Future

THE 1-2-3 OF BIOMETRICS-ENABLED IDENTIFICATION IN TRAVEL

PRE-DEPARTURE

AIRPORT

DOCUMENT READ & AUTHENTICATION

STEP 1

OPTICAL CHARACTER RECOGNITION (OCR)



SMARTPHONE CAMERA READS MACHINE READABLE ZONE (MRZ) FROM DOCUMENT

NEAR FIELD COMMUNICATION (NFC)



SMARTPHONE INTERACTS WITH DOCUMENT CHIP

AUTHENTICATION



DOCUMENT IS AUTHENTICATED (I.E. PUBLIC KEY DIRECTORY/CBSA TRAVEL DOCUMENT VERIFICATION SERVICE)

BIOMETRIC IDENTITY VERIFICATION

STEP 2

TAKE SELFIE

A



QUALITY ASSESSMENT

B

Quality of selfie (ISO 39794-5)

- INTEROCULAR DISTANCE
- HEAD POSITION
- ARTIFACTS IN IMAGE
- FACE OCCLUSIONS (E.G. GLASSES, MASKS, HEAD SCARFS)
- ILLUMINATION, FOCUS, ETC...

FRAUD DETECTION

C

Assess threat vectors (ISO 30107-3)

- LIVENESS
- PRESENTATION ATTACK (SPOOFING WITH MASKS, PICTURES, ETC)
- DIGITAL AND HARDWARE INJECTION ATTACKS (INCLUDING DEEP FAKES)

1:1 MATCHING VERIFICATION

D

Template: compare (ISO 19795-1)



BIOMETRIC IDENTITY RESOLUTION (TOUCHLESS)

STEP 3

TAKE PHOTO

A



REPEAT

B & C

1:FEW MATCHING (IDENTIFICATION ISO 19795-1)

D

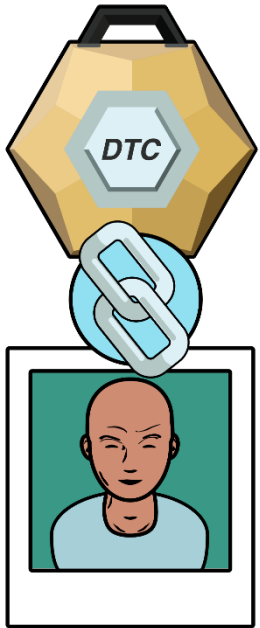
Gallery of expected individuals



- SUBMITTED IN ADVANCE
- DELETED AFTER IDENTIFICATION

VIEWING AND AUTHENTICATING PASSPORT DATA

VERIFYING IDENTITY



Borders and Biometrics of the Future

In order for biometric matching to yield border management with opportunities to automate and redeploy resources, it is important to:

- Understand how the technology is operating (e.g., demographic differentials, system errors/thresholds, etc.);
- Collaborate with stakeholders in the continuum that feed into your processes (e.g., image capture and data quality);
- Set thresholds for touchpoints in line with the level of risk (e.g., will you see that traveller in person?); and
- Manage the entire biometric system.

Cannot take a set-it-and-forget-it approach to managing a biometric system.

Thank You

