The Path to Digital Identity: Principles for Mobile Identity Credentials

Tuesday, October 20, 2020, 2:30 pm ET

Presented by:

IBIA

BIOMETRIC UPDATE.COM

Speakers

Chris Burt
Editor
Biometric Update

Justin Ikura
Deputy Director, Passport Program Policy, Admissibility Immigration, Refugees and Citizenship Canada / Government of Canada

Jean-Baptiste Milan
Mobile ID Product Director – goID™ Citizen ID Solutions, HID Global

Melinda (Mindy) Stephens
Manager, Identity Management
AAMVA (American Association of Motor Vehicle Administrators)

Paul J. Townsend, CISSP
Business Development, Federal Systems, Acuant

IBIA

BIOMETRIC
UPDATE.COM

The State of Mobile Identity Credentials

The Path to Digital Identity: Principles for Mobile Identity Credentials

- The transition to mobile identity credentials has been a key objective for several years. As the digital world has expanded, the many limitations of physical documents have become apparent. Today, the need for mobile identity credentials is even more immediate as COVID-19 has underscored the critical health importance of contactless means of establishing identity. With technology advances, mobile identity credentials have begun to support a broad range of contactless and digital use cases, including ecommerce, online banking, trust service providers, border management, contactless travel, and other transactions that require a high level of identity assurance.

The State of Mobile Identity Credentials

The Path to Digital Identity: Principles for Mobile Identity Credentials

- This webinar will address the incorporation of biometrics and significant privacy-protecting security processes that allow mobile credentials to be authenticated and trusted to the same extent as the physical document. Please join IBIA and Biometric Update in this first webinar that addresses ”*The Path to Digital Identity: Principles for Mobile Identity Credentials*” with key leaders in the industry.

IBIA

BIOMETRIC
UPDATE.COM

IBIA

International
Biometrics+Identity
Association

IBIA.ORG

BIOMETRIC
UPDATE.COM

biometricupdate.com

IBIA

International Biometrics+Identity Association

Identity Matters

The Path to Digital Identity: Principles for Mobile Identity Credentials

October 20, 2020

Jean-Baptiste Milan
Mobile ID Product Director – goID™
Citizen ID Solutions, HID Global

Paul J. Townsend, CISSP
Business Development, Federal
Systems, Acuant

Subject

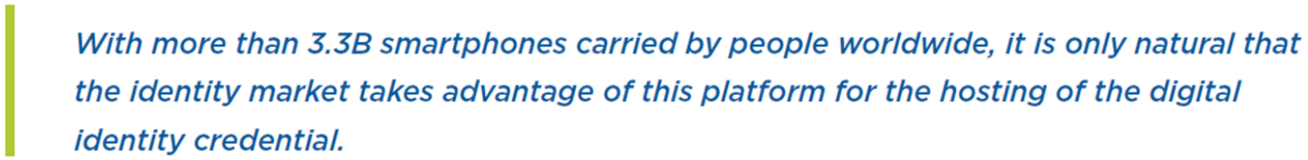
- This paper examines the transition from the use of physical identity documents to digital identity credentials, specifically related to driver licenses and travel documents.
- It provides a discussion of the principles that must be addressed from the establishment of the biometrically enabled digital credential within a mobile device to its use in any biometrically reliant identity authentication process.

Authors

- Paul Townsend, Acuant
- Bill Dumont, Innovatrics
- Magruder Dent, Aware
- Jean-Baptiste Milan, HID Global
- Tovah Ladier, IBIA

Core Principles

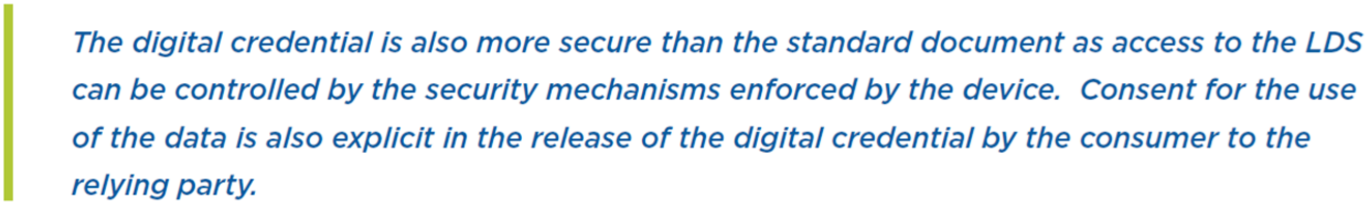
- Digital Credentials will Assert the Same Identity and Privileges as the Credential from which they are Derived
- International Standards provide Interoperability & Trust
- Use of Biometrics is Foundational to Any Credential
- Self-Service Requires Robust Document Authentication
- FRM Processes are Inherently Critical to Success



> *With more than 3.3B smartphones carried by people worldwide, it is only natural that the identity market takes advantage of this platform for the hosting of the digital identity credential.*

Advantages of Digital Credentials

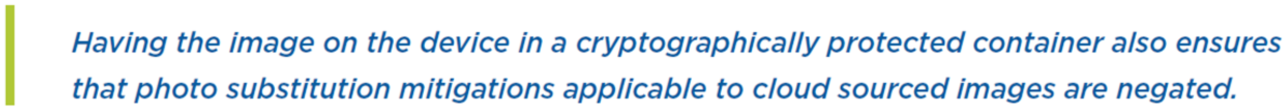
- Standards for Data Integrity, Interoperability, & Communications have been Defined
- Support a Wide Range of Use Cases
- Enable Risk Mitigation, Consent, & Privacy by Design



The digital credential is also more secure than the standard document as access to the LDS can be controlled by the security mechanisms enforced by the device. Consent for the use of the data is also explicit in the release of the digital credential by the consumer to the relying party.

Implementation Considerations

- Credential Authentication Mechanisms
- Enrollment Methodology
  - In-Person
  - Remote Self-Service
- Data Protections and Privacy Controls

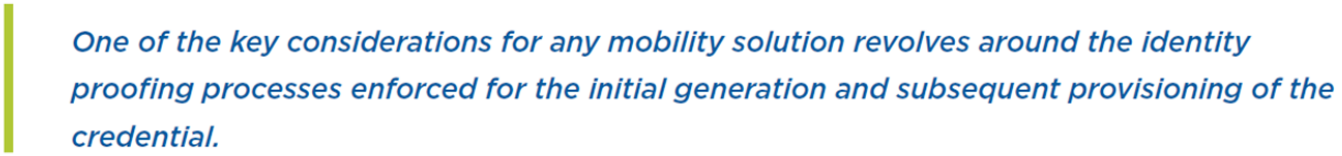


> *Having the image on the device in a cryptographically protected container also ensures that photo substitution mitigations applicable to cloud sourced images are negated.*

Life Cycle Process 1:

Unattended/Remote Vetting & Digital Identity Provisioning

- Identity Proofing Establishes the Trust Anchor
- Biometrics Bind the Individual to the Trust Anchor
- Digital Credential Delivery



One of the key considerations for any mobility solution revolves around the identity proofing processes enforced for the initial generation and subsequent provisioning of the credential.

Life Cycle Process 2:

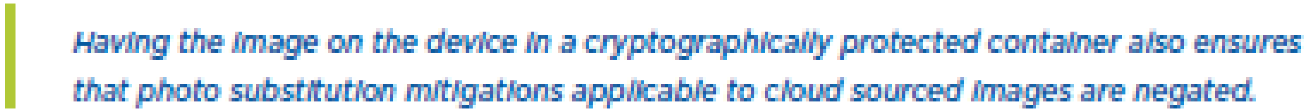
Biometric Capture and Authentication

- Frictionless Capture
- Identity Assurance

The registration and delivery processes for DTCs can take several forms, based on the mechanisms allowed by the Issuing State.

Life Cycle Process 3:
Store Biometrics

- Image Quality Controls
- Data Protection Mechanisms
- Access Control Mechanisms
- Privacy by Design and Consent Mechanisms



> *Having the image on the device in a cryptographically protected container also ensures that photo substitution mitigations applicable to cloud sourced images are negated.*

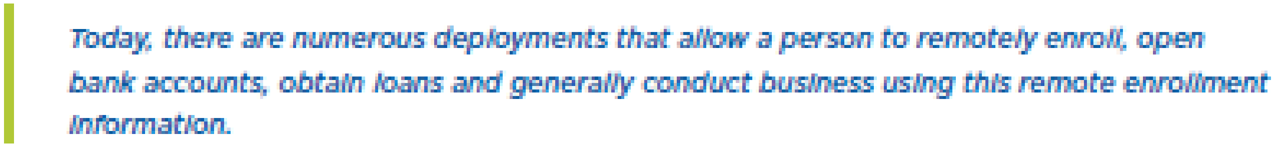
Life Cycle Process 4:
Share Biometrics

- Self-contained versus Distributed Workflows
- Trust Framework Supports Secure Sharing of Biometrics

> *Digital credentials can provide a thoroughly vetted identity assertion as well as support the presentation of only the data necessary to complete a given transaction.*

Physical versus Digital

- Data Privacy
- Identity Authentication



Today, there are numerous deployments that allow a person to remotely enroll, open bank accounts, obtain loans and generally conduct business using this remote enrollment information.

Conclusion

- Supporting Technologies and Trust Frameworks Exist to Support each of these Principles
- Principles provide a Sound Basis for the Implementation and Use of Biometrically Based Processes
- Proper Design Ensures Trust, Data Integrity, and Privacy throughout the Life Cycle of the Digital Credential

IBIA

International
Biometrics+Identity
Association

Identity
Matters

For more info,
visit us at ibia.org

American Association of
Motor Vehicle Administrators

Mobile Driver License (mDL)

IBIA Webinar October 2020

Melinda (Mindy) Stephens
Manager, Identity Management
AAMVA (American Association of Motor Vehicle Administrators)

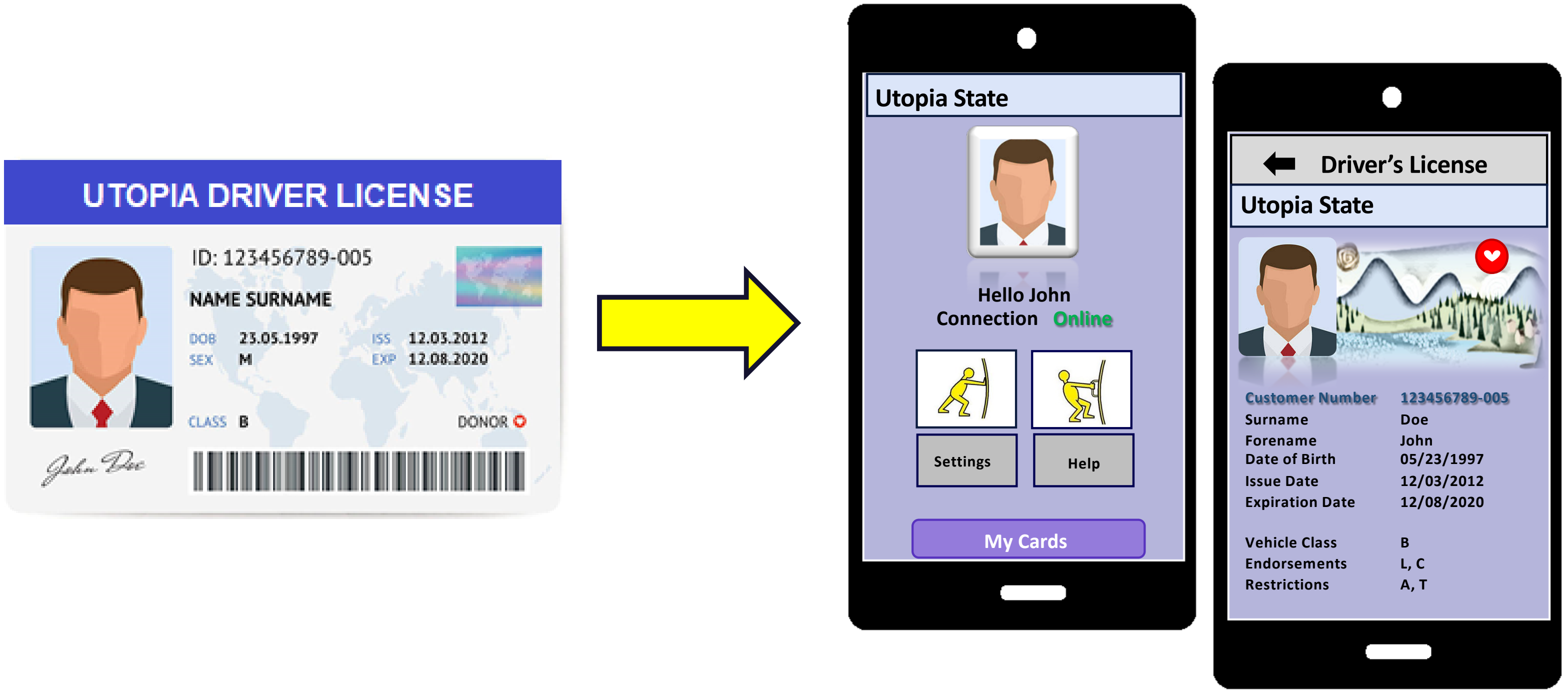
OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

Agenda

- ❑ mDL Overview
  - What is mDL?
  - What mDL is not
  - mDL Concept
  - Where mDL will be used
  - Functional Requirements
- ❑ Benefits of mDL

What is mDL?



UTOPIA DRIVER LICENSE

ID: 123456789-005

NAME SURNAME

DOB	23.05.1997	ISS	12.03.2012
SEX	M	EXP	12.08.2020

CLASS B

DONOR

John Doe

Utopia State

Hello John
Connection Online

Settings

Help

My Cards

Driver's License

Utopia State

Customer Number	123456789-005
Surname	Doe
Forename	John
Date of Birth	05/23/1997
Issue Date	12/03/2012
Expiration Date	12/08/2020
Vehicle Class	B
Endorsements	L, C
Restrictions	A, T

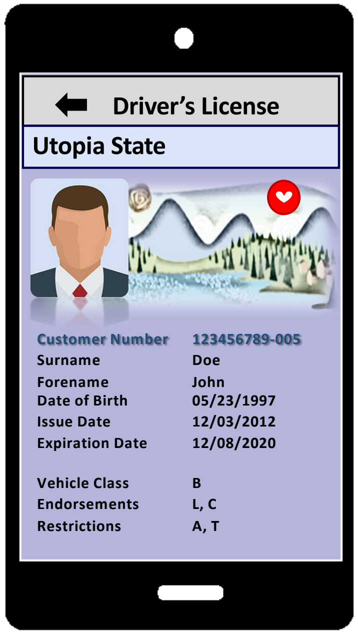
What an mDL is not…

UTOPIA DRIVER LICENSE
ID: 123456789
NAME SURNAME
DOB
SEX
ISS 12.03.2012
EXP 12.08.2020
DONOR

mDL is NOT a picture of the physical license on the device

Relying Party will NOT need to touch/take the holder’s device

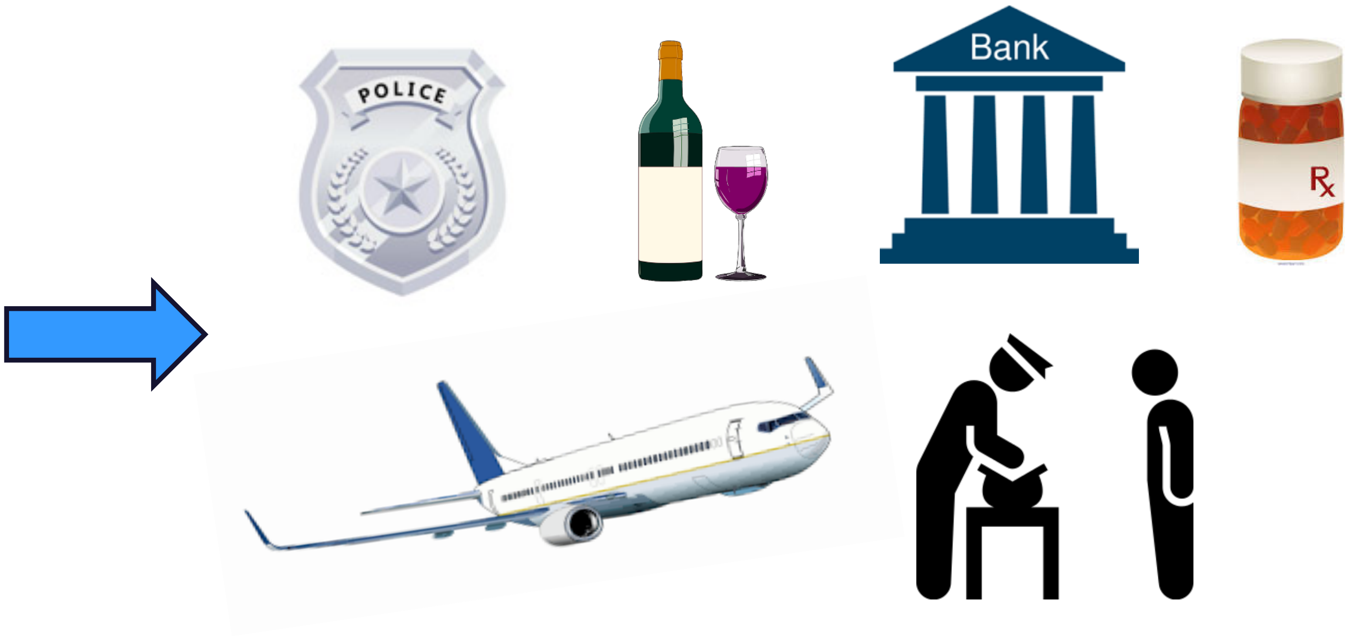
mDL Use



Driver's License

Utopia State

Customer Number	123456789-005
Surname	Doe
Forename	John
Date of Birth	05/23/1997
Issue Date	12/03/2012
Expiration Date	12/08/2020
Vehicle Class	B
Endorsements	L, C
Restrictions	A, T



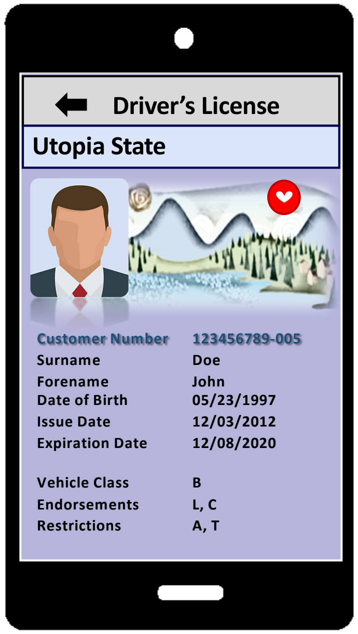
Functional Requirements

Confirm Identity

Convey Driving Privileges

Trustable

Interoperable



Driver's License

Utopia State

Customer Number	123456789-005
Surname	Doe
Forename	John
Date of Birth	05/23/1997
Issue Date	12/03/2012
Expiration Date	12/08/2020
Vehicle Class	B
Endorsements	L, C
Restrictions	A, T

Selective Info Release

Attended and Unattended

Remote Management

Work Offline

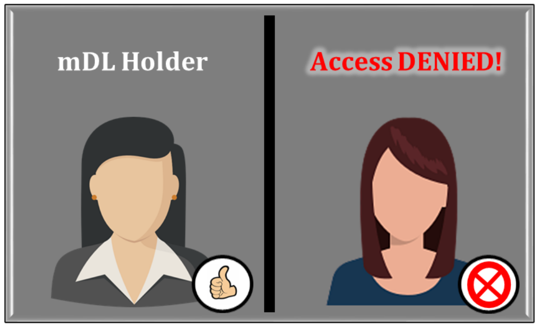
Privacy and Security By Design

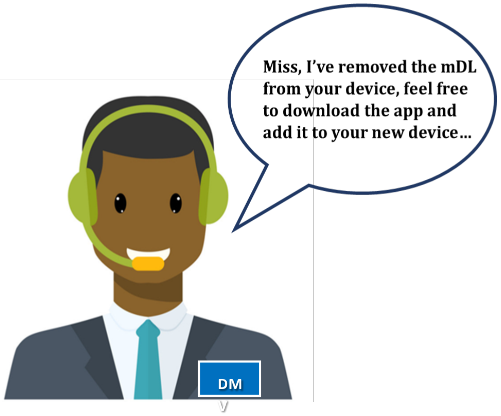
Benefits of mDL

No lost/stolen mDL

Physical Credential

mDL




Miss, I've removed the mDL from your device, feel free to download the app and add it to your new device…
DM

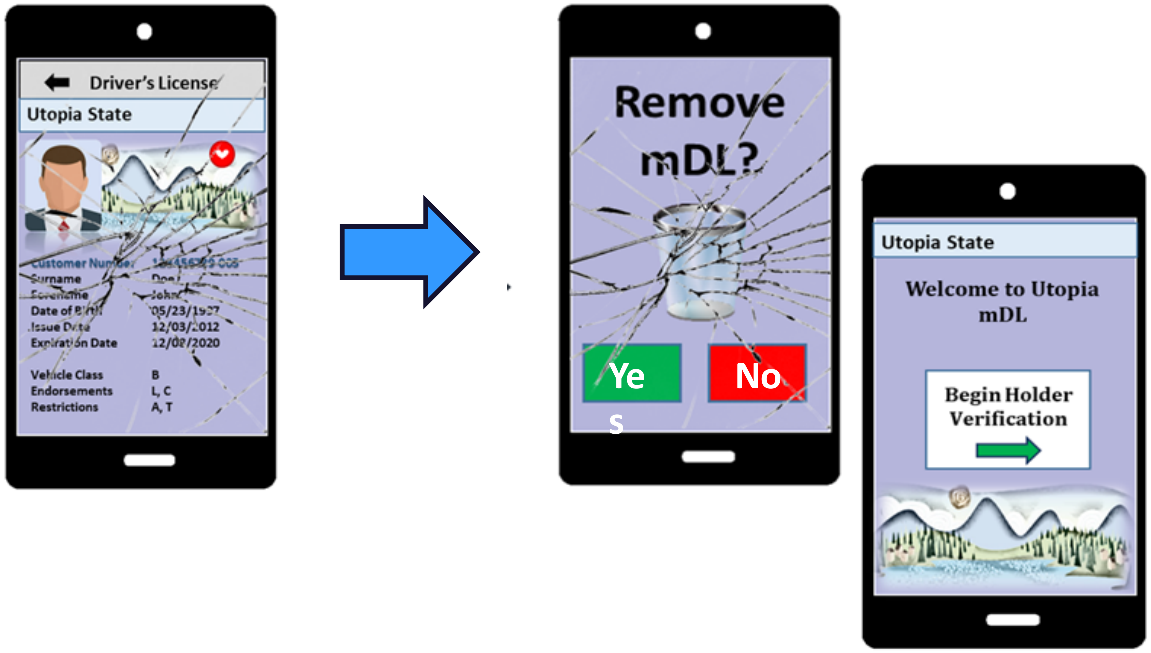
Functionality and Features shown on this slide are subject to the IA's design and policies. Not defined in the standards.

Cannot damage mDL

Physical Credential

DRIVER LICENSE
AB 123456789-005
NAME SURNAME
Lorem ipsum,
Dolor sit amet, 12354
DOB 21.05.1987
SEX F
ISS 12.05.2017
EXP 12.08.2027
CLASS B

mDL



Driver's License

Utopia State

Customer Number 123456789 005
Surname Doe
Forename John
Date of Birth 05/23/1987
Issue Date 12/03/2012
Expiration Date 12/08/2020

Vehicle Class B
Endorsements L, C
Restrictions A, T

Remove mDL?

Yes No

Utopia State

Welcome to Utopia mDL

Begin Holder Verification

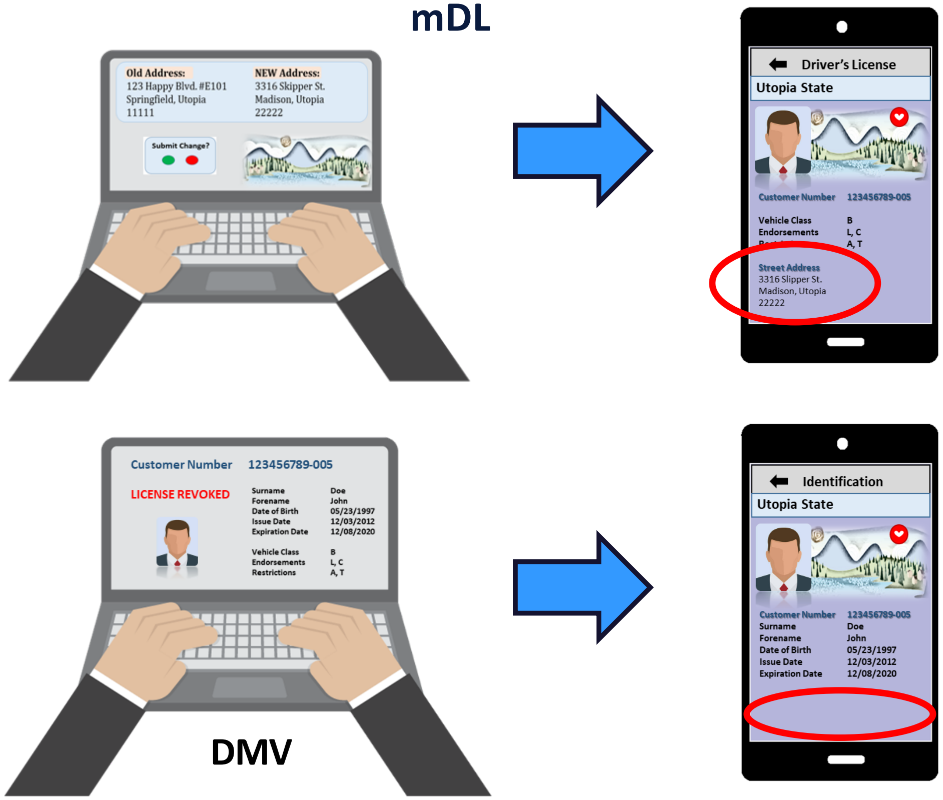
Functionality and Features shown on this slide are subject to the IA's design and policies. Not defined in the standards.

Real time updates

Physical Credential

Your license says you live in Springfield not Madison...

mDL



Old Address:
123 Happy Blvd. #E101
Springfield, Utopia
11111

NEW Address:
3316 Skipper St.
Madison, Utopia
22222

Submit Change? ● ●

Driver's License

Utopia State

Customer Number	123456789-005
Vehicle Class	B
Endorsements	L, C
Restrictions	A, T

Street Address
3316 Slipper St.
Madison, Utopia
22222

Customer Number	123456789-005

LICENSE REVOKED

Surname	Doe
Forename	John
Date of Birth	05/23/1997
Issue Date	12/03/2012
Expiration Date	12/08/2020
Vehicle Class	B
Endorsements	L, C
Restrictions	A, T

Identification

Utopia State

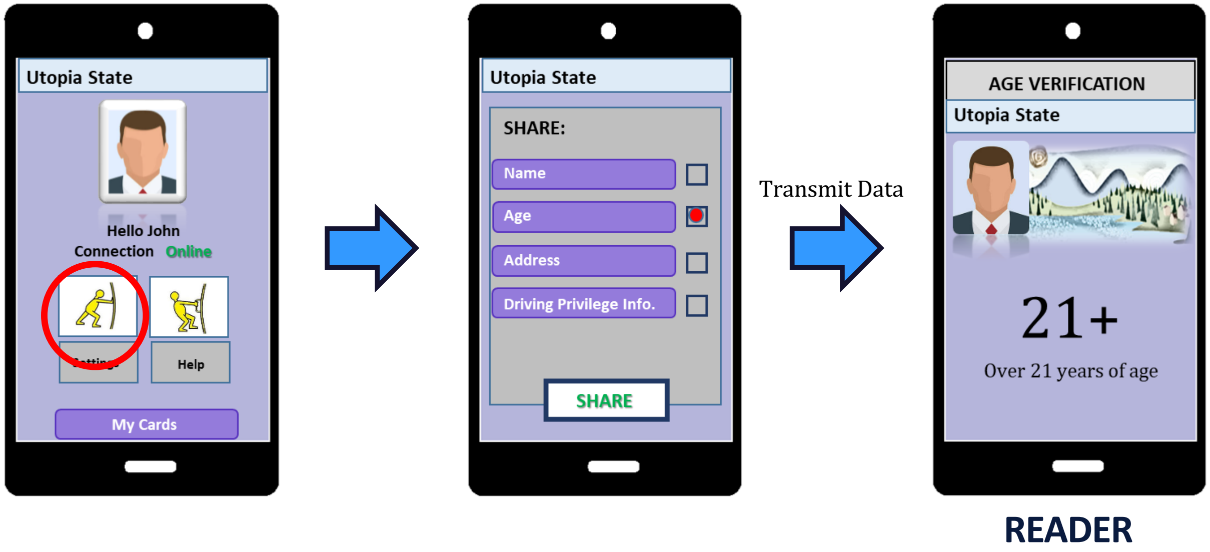
Customer Number	123456789-005
Surname	Doe
Forename	John
Date of Birth	05/23/1997
Issue Date	12/03/2012
Expiration Date	12/08/2020

Functionality and Features shown on this slide are subject to the IA's design and policies. Not defined in the standards.

Privacy Protection

Physical Credential

mDL

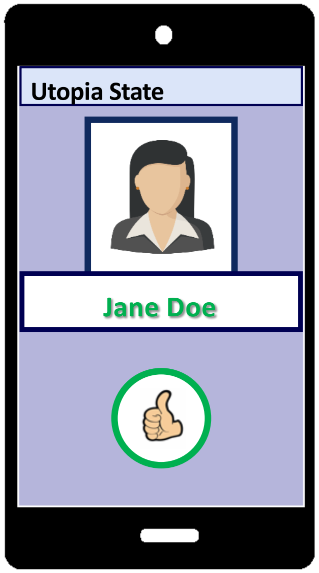


Functionality and Features shown on this slide are subject to the IA's design and policies. Not defined in the standards.

Goodbye Flash Pass

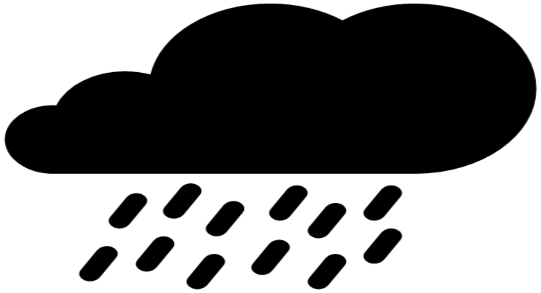
Physical Credential

mDL



Functionality and Features shown on this slide are subject to the IA's design and policies. Not defined in the standards.

mDL means fewer counterfeits



Contact Information

Mindy Stephens

mstephens@aamva.org

571.201.3472

The Digital Travel Credential: *A Secure/Interoperable Identity Container*

Justin Ikura

Vice Chair, International Civil Aviation Organization (ICAO) New Technologies Working Group (NTWG)

Presentation Overview

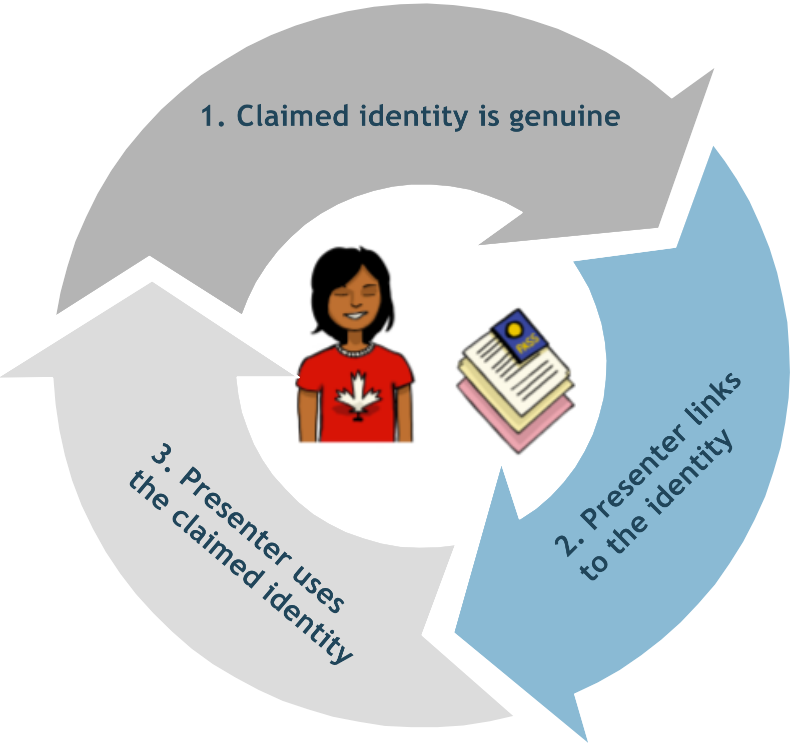
1. Passport Issuance and ID
   a. The role of biometrics
   b. Exporting the biometric

2. The ePassport

3. The Digital Travel Credential

(1) Passport Issuance and Identity

Establishing Identity at Issuance

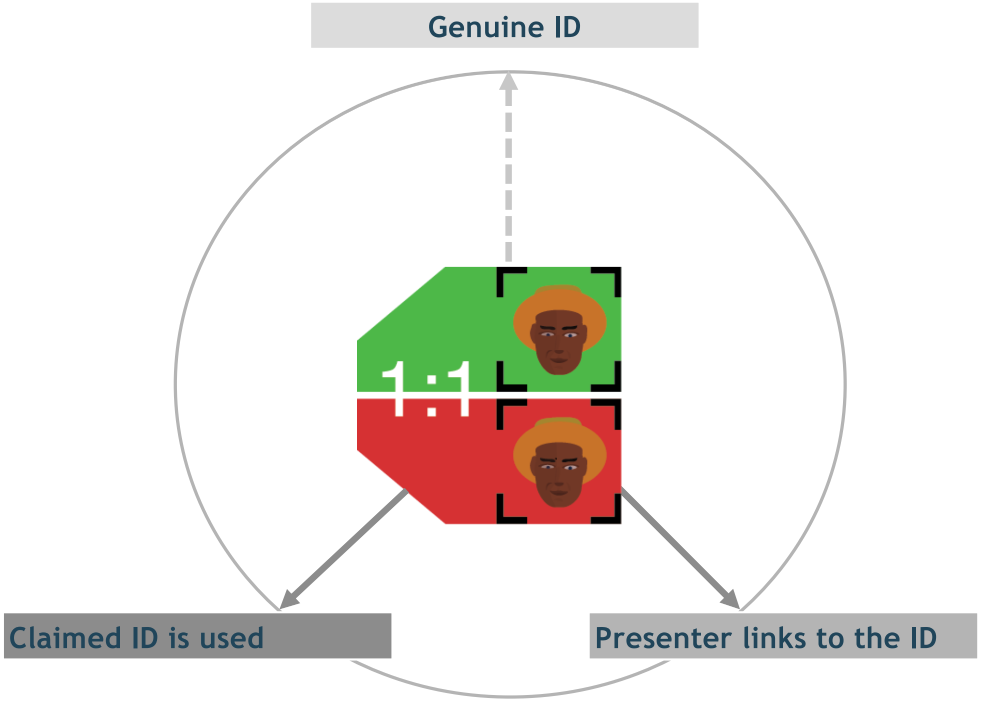

1. Claimed identity is genuine
2. Presenter links to the identity
3. Presenter uses the claimed identity

- Identity is a combination of biometric and biographic attributes.

- Establishing an identity is therefore a straight-forward process…?
  - Verify the attributes (often contained in documents); and
  - Associate them to the individual.

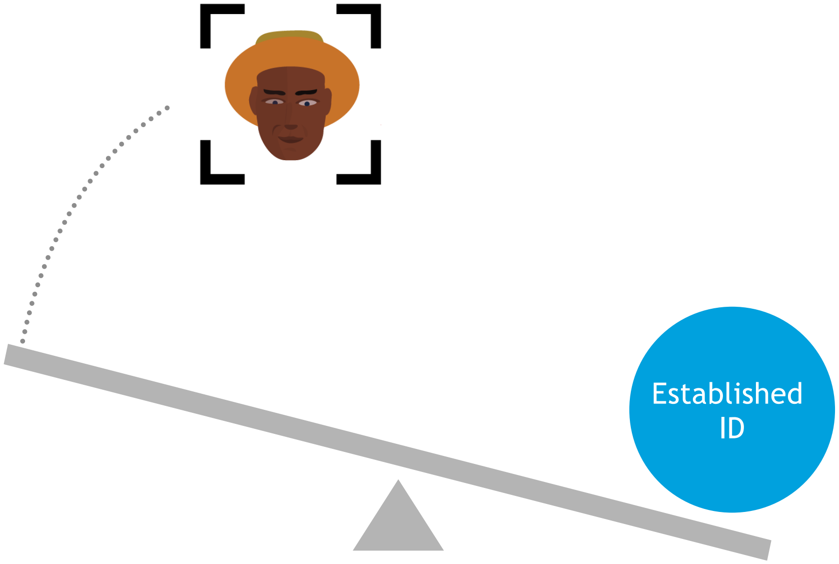
- From the passport issuance perspective, identity establishment is a far more complex process:
  - Identity evolves (people may move, marry, etc..);
  - Identity is linked to a community; and
  - Identity can be assumed…

Biometrics Can Play A Role



- Biometrics play a more significant role in elements 2 and 3.
- Biometrics are used to match an applicant to the claimed ID, seek-out endorsement from the community, and ensure that ID is not owned by someone else.
- This matching can be manual (i.e., signing photos) and/or automated (i.e., facial recognition).

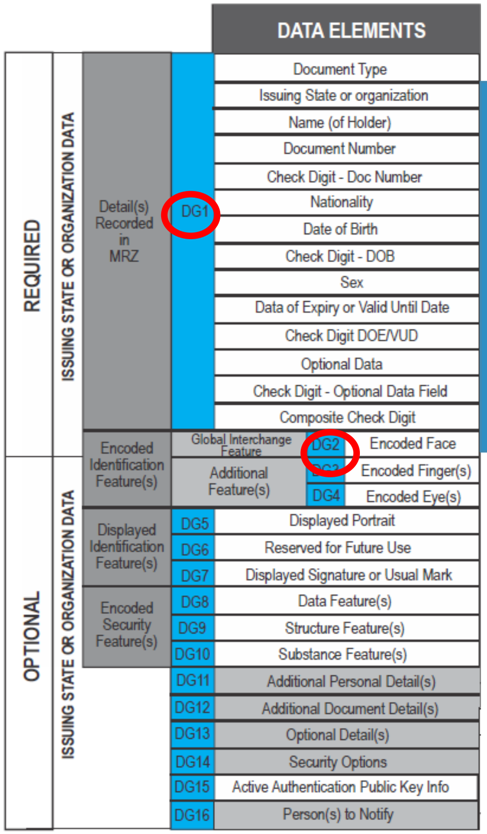
Exporting the biometric



- Once the applicant’s ID is established, the biometric can confidently be added to the passport.
- Puts traveler’s in a position to assert their ID with a trust-worthy biometrically-enabled token.

(2) The ePassport: A Key Building Block

ePassport Chip Contents



					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

Data Group 1 (DG1)

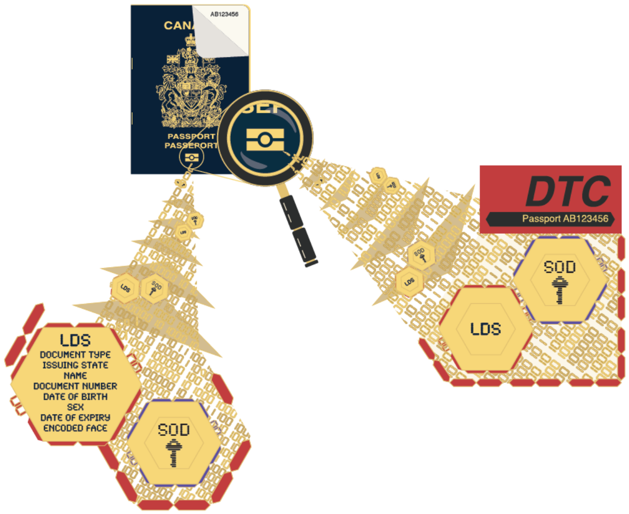
- Issuing Organization
- Name of Holder
- Document Number
- Nationality
- Date of Birth
- Sex
- Date of Expiry…

Data Group 2 (DG2)

- Face

Data is added and encrypted at the time of issuance

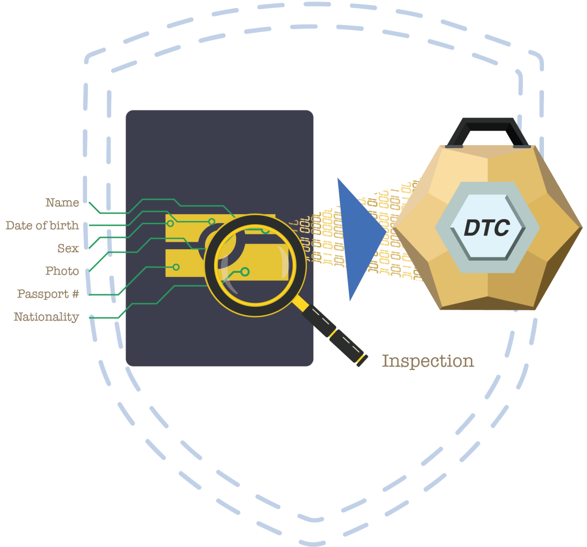
What did we effectively want to achieve and why?



- Passport data is used by a range of actors in the travel continuum:
  - **Immigration authorities** to issue travel authorizations (e.g. electronic authorities, visas, etc.)
  - **Transport Ministries or agencies** to support identity management and aviation security.
  - **Air industry** to fulfill transporter obligations and manage travelers.
  - **Border control** to pre-screen travelers, identify lost/stolen books and identify travelers.
- The principle objective of the DTC Sub-Group was to make this data accessible without physical presentation of the passport.

(3) The Digital Travel Credential (DTC)

High-Level Explanation

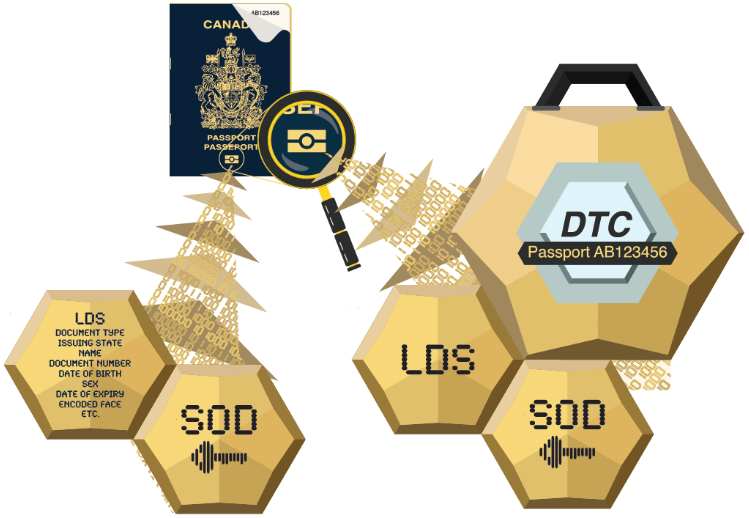


- The sub-group has determined that a DTC could be created in two ways: as a derivative of the ePassport (i.e. extracted data); and/or issued in parallel to or in replacement of a physical ePassport.

- The DTC would contain the facial image, the holder's personal details, and the security features to support authentication.

- All generations of the DTC will be backwards compatible.

Pulled from a [Physical] Passport



- **Digital copy + physical book:** Data is extracted from the physical ePassport; holder must carry the physical travel document as back-up.

- Data extraction can be done today; however:
  - To be useful, data must stored in a mobile and globally interoperable container; and
  - Like an ePassport, data should be authenticated before it can be applied.

- Once the data is authenticated, the DTC can be trusted to support passenger identification (i.e. biographic checks and facial matching).

Pulled from a Passport Record (v1)

CANAD
AB123456
PASSPORT
PASSEPORT
LDS
SOD
DTC
Passport AB123456
LDS
DOCUMENT TYPE
ISSUING STATE
NAME
DOCUMENT NUMBER
DATE OF BIRTH
SEX
DATE OF EXPIRY
ENCODED FACE
ETC.
SOD

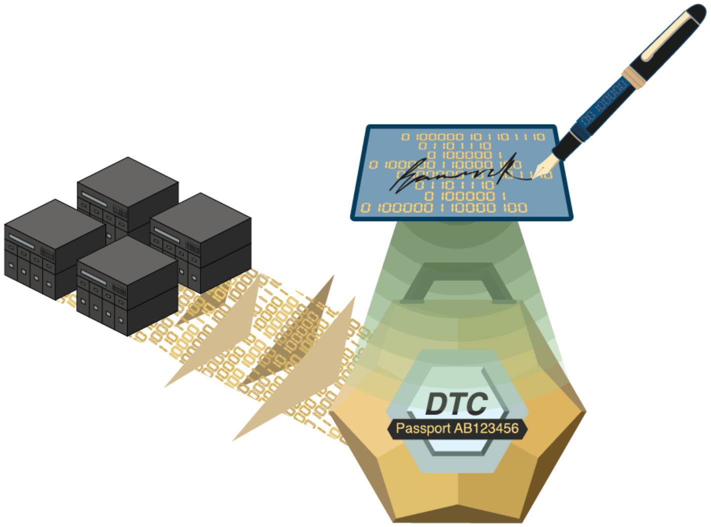
- **Digitally signed copy + physical book:** Data is extracted from the issuer database and digitally signed by the issuing authority; the DTC digital container is the primary back-up, physical book is an alternate back-up.
- Difference between generation 1 and generation 2 is the active role of the issuing authority to issue and secure the digital container.
- Beginning to look at medium- to long-term solutions.

Pulled from a Passport Record (v2)

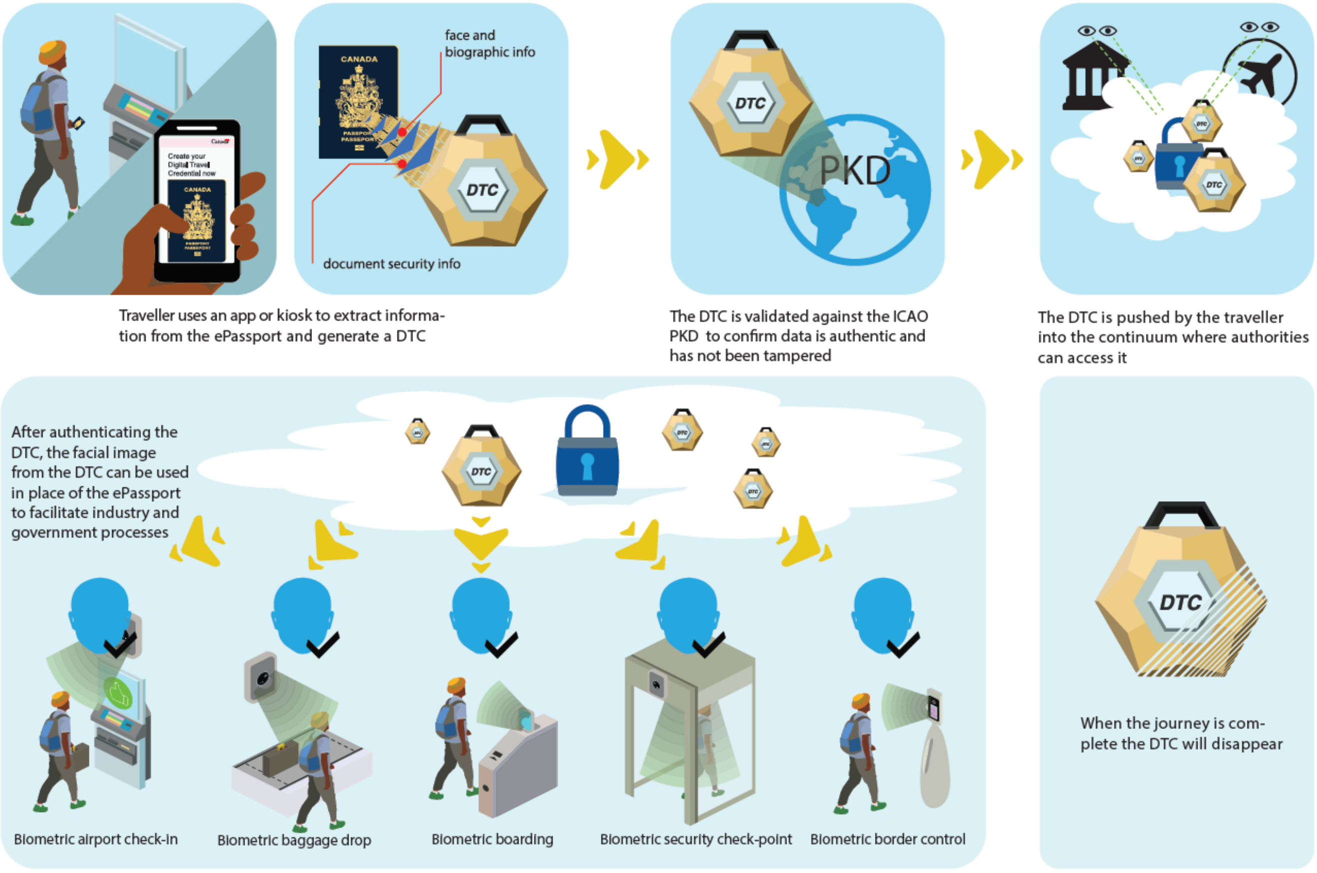
- **Issued DTC; no physical book:** Passport authority issues a digitally signed DTC; the smart device serves as the fall-back.

- The “physical” book is replaced by a digital container, which may be queried to determine whether traveler holds the original source of data.

- This is the long-term solution.



How could a DTC be used?



Traveller uses an app or kiosk to extract information from the ePassport and generate a DTC

The DTC is validated against the ICAO PKD to confirm data is authentic and has not been tampered

The DTC is pushed by the traveller into the continuum where authorities can access it

After authenticating the DTC, the facial image from the DTC can be used in place of the ePassport to facilitate industry and government processes

When the journey is complete the DTC will disappear