The Path to Digital Identity: Principles for Mobile Identity Credentials

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

- 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
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
Identity Matters

For more info, visit us at ibia.org
Mobile Driver License (mDL)

IBIA Webinar October 2020

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

UTOPIA DRIVER LICENSE

Hello John
Connection Online

My Cards
Settings Help

Driver's License

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

OUR VISION
Safe drivers | Safe vehicles | Secure identities | Saving lives!
mDL is **NOT** a picture of the physical license on the device

Relying Party will **NOT** need to touch/take the holder’s device
Confirm Identity
Convey Driving Privileges
Trustable
Interoperable

Selective Info Release
Attended and Unattended
Remote Management
Work Offline

Privacy and Security By Design

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

O U R  V I S I O N
Safe drivers  |  Safe vehicles  |  Secure identities  |  Saving lives!
Benefits of mDL
No lost/stolen mDL

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

Cannot damage mDL

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

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

DMV

mDL

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

She’s cute. Wonder if she lives nearby...?

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

mDL

Our Vision

Safe drivers | Safe vehicles | Secure identities | Saving lives!
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
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 straightforward 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 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)
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)

- **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.
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?

1. Traveller uses an app or kiosk to extract information from the ePassport and generate a DTC.
2. The DTC is validated against the ICAO PKD to confirm data is authentic and has not been tampered.
3. After authenticating the DTC, the facial image from the DTC can be used in place of the ePassport to facilitate industry and government processes.
4. The DTC is pushed by the traveller into the continuum where authorities can access it.
5. When the journey is complete, the DTC will disappear.