



International  
**Biometrics+Identity**  
Association

# Principles for the Implementation and Use of Biometrically Enabled Mobile Identity Credentials



**The International Biometrics + Identity Association (IBIA) is the leading voice for the biometrics and identity technology industry. It advances the transparent and secure use of these technologies to confirm human identity in our physical and digital worlds. #identitymatters**

REFERENCES: ISO 18013-5, ICAO DTC, ISO 23220, IBIA privacy principles

© 2020 International Biometrics + Identity Association

# Executive Summary

## 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.

## Core Principles:

- **Digital credentials will assert the same identity and requisite privileges as the physical credential from which they are derived.**

1. A Mobile Driver License (mDL) will assert that the Issuing State has granted the asserted identity the permission to drive. A Digital Travel Credential will assert that the citizen identity has been vetted by the Issuing State and that the digital credential is allowed border crossing authorizations equal to those supported by the physical ePassport document.
2. This foundational principle requires a focus on the security processes supporting the life cycle of the digital credential. Details are important in the methods and mechanisms that are used to derive or digitize the identity data from the original physical document or the authoritative identity database. Protection mechanisms and access controls must be built in – from the establishment of the trust anchor to its use as the basis for biometrically enabled transactions. Consent mechanisms are important for the release of only the minimum amount of private data needed from the digital credential to support the transaction. To support these security mechanisms, a robust trust framework must be leveraged.
3. These security considerations are now well supported due to the quality and ubiquitous use of mobile devices worldwide, and the supporting identity trust fabrics that exist globally. Moving from the use of physical documents to an equivalent digital credential provides convenience to the user, and strong identity assurance mechanisms to the relying party.

- **Adherence to internationally accepted standards definitions of the credential and its contents.** The protection and access mechanisms defined within these standards ensure the global trust and interoperability of these digital credentials. While physical document authenticity and identity integrity protections exist for physical documents, these same principles are addressed by the standards-based protections and processes that have been defined for their digital equivalents. These mechanisms are used to establish and maintain trust in the digital credential; to ensure the data integrity and privacy of its contents; and to support its use across many diverse use cases. International standards are required throughout the entire credential life cycle from enrollment to issuance to usage.
- **Use of biometrics is foundational to any identity credential – physical or digital.** A printed facial image is the standard rendering on the front of an identity document that is used to associate the biographic information with an individual. An electronic image provides that same linkage within the digital credential. Standard formats are used so that biometric facial recognition matching (FRM) processes can be supported using this image to determine the match of the individual to the credential. Whether the biographic data is extracted from an authoritative database or derived from an existing credential, its linkage to the individual is a key principle that must be enforced in any digital credential program.
- **Self-service processes require robust document authentication processes to establish the authenticity of the source identity document.** These processes may include the evaluation of the physical security features found on the face of the document, as well as the cryptographic assessment of the contents of the electronic chip of an ePassport.
- **FRM processes are inherently critical to the success of a digital credential program.** This biometric assessment provides the linkage necessary to establish the trust anchor (the digital identity credential). It binds the biographic data from the authenticated document to the individual presenting the document. It allows the digital credential to be trusted globally and granted the same authorizations and privileges as the physical document. It allows for the real-time assessment of the person presenting the digital credential as the trusted individual asserted by the biometric contained within that credential.

*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.*

## Conclusion:

The supporting technologies and trust frameworks exist to support each of these principles. While not comprehensive and exhaustive of all the principles that must be addressed by a digital identity credential program, the principles presented in this paper provide a sound basis for the implementation and use of biometrically based processes to ensure trust, data integrity, and privacy throughout the life cycle of the digital credential.

## Overview

As with many cards in our wallets, US driver licenses are migrating to Mobile Driver Licenses (mDL) which are electronic equivalents of our current physical driver licenses securely stored on our mobile devices. This migration is also occurring with other identification documents such as ePassports and their digital equivalent, the Digital Travel Credential (DTC).

This concept has been around for years but has only recently been fully explored based on the advancement of several technologies. Digital Identity solutions are now feasible due to the enhanced quality of the mobile devices on the market, the advancement of biometric technologies to be employed on small footprint devices, the availability of cloud services to support critical vetting and authentication processes, and the worldwide acceptance of the supporting use cases.

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

A Digital Credential is an electronic representation of a physical identity document that can be stored on a mobile device.

The data from the source physical document is digitized and securely provisioned to a mobile device so that it can easily be presented and authenticated by any relying party. The digital credential (or electronic identity trust anchor) is meant to assert the identity and associated privileges of the holder with the equivalency of the physical identity document.

As government agencies move to digital credentials, convenience and security are of utmost importance. Convenience is realized by not having to extract your credential from your wallet. A digital credential offers a frictionless approach for consumers interacting with government services. Security of the digital credential is ensured by linking the credential holder to the digital credential through the incorporation and binding of biometrics into the credential. This cryptographic binding establishes a trusted identity anchor that can then be used in place of the physical document. For mobile credentials, the facial biometric is the logical choice since the photograph is already present on the document.

### **Applicable international standards have been defined for data integrity, interoperability, and communications**

At the same time, applicable international standards have also been developed to address the interoperability and common interfaces for protecting, retrieving, and authenticating the data, including:

- ISO 18013-5 for Mobile Driver Licenses (mDLs)
- ICAO 9303 / ISO 7501 for ePassports and Digital Travel Credentials (DTCs)

*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.*

The data contained in either of these digital credentials is organized in a standardized Logical Data Structure (LDS) and digitally signed, using the Issuer's Public Key Infrastructure (PKI), to cryptographically protect the privacy data contents. These protections

- ensure interoperability and data integrity over time
- prove the authenticity of the credential when it is being used
- support biometric verification that the presenter of the credential is its owner.

These standards also address the communication mechanisms and protections to be employed for accessing and releasing the data from the device. Communications between the digital credential and the reader of the credential are cryptographically protected. The data is expected to be held within the most secure container available to the device so that its integrity is ensured, and this may include encryption of the data at rest, if required. The data release controls specified in the standards also enable the mobile phone owner to control who has access to the data in the LDS.

Relying Party communication with the device can leverage the multiple communication interfaces inherent in any mobile device, including NFC, Bluetooth, WIFI or barcode readers. This provision in the standards allows the developers of relying party applications to use the most effective interface for their target deployment environment.

### **Digital credentials support a wide range of use cases**

As important as the protection of the data, the ISO standard interface to the LDS allows the credential to be used to support a wide range of use cases, including point of sale, roadside police stops, border crossings, remote financial account provisioning, and other use cases. In each case, the credential owner controls the personal information shared with each application. For example, when purchasing alcohol in the USA, the user can leverage their mDL to only display the photograph and the date of birth. No unnecessary personal information such as one's street address needs to be shared.

### **Digital credentials enable risk mitigation, consent, and privacy by design processes**

Another advantage to the use of the digital credential is that it allows the relying party to do a manual comparison of the credential holder to the actual photograph appearing on the reader screen – just as is currently done with a physical document. Digital credentials now allow the automation of this manual process, and the incorporation of risk mitigating measures. Using an automated, technology enhanced process can provide a higher level of assurance in the authenticity of the credential and the person presenting it. This significantly reduces the risk to the relying party in any use case.

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**

There have been standards set by country and/or state for a physical driver's license regarding the incorporation of physical security features that allow them to be assessed as authentic. In order to move to a digital credential that can similarly be assessed, we must first understand if the same or different standards have been established. For instance, today drivers' licenses often have watermarks, holograms and other specific security markings that can be read by a document reader to assure their presence. In addition, certain fields must be in specific areas of a physical ID (i.e., picture, biographical information, descriptive physical information, etc.).

With physical documents, the quality of the encoding of the physical security features is critical to the assessment that the ID is both authentic and has not been tampered with. Similar encoding and security controls are defined in the governing standards for digital credentials. Automated enforcement mechanisms exist for a relying party to easily assess the authenticity and integrity of the physical document. The relying party to the transaction can leverage these

*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.*

mechanisms to ensure that the document was issued by a trusted issuer and has not been modified since its encoding.

This trust framework allows for a similar assessment of the digital credential (or eID) and the subsequent granting of privileges to the eID that, to this point, have been tied to the physical document. The digital credential can be used to assert that a person has certain privileges that support actions such as driving, the purchase of alcohol or pharmaceuticals, and even access to a certain controlled perimeter, either physical or logical. If this eID is used for other applications like airport entry, not only the states but the Federal government must approve of the credential, and its supporting trust framework, to have confidence in both its authenticity and the binding of the individual to the credential.

### **Enrollment Methodology – In-Person or Remote Self-Service**

In order to establish any trusted identity, one must consider the enrollment method. One of the advantages of eIDs is the ability to remotely enroll an individual, lessening the costs or employee overheads that are needed for the vetting processes as well as the production and personalization of the physical IDs. Today it's possible to take a selfie and compare that to a picture in an existing database or document. However, there must be an acceptable level of security enforced to assure that the enrollment is being done of a live person, not spoofed by a picture or set of fingerprints that were obtained prior to the enrollment and then used to defraud the agency honoring the final document.

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. However, as mentioned earlier, the establishment of a digital credential may require additional risk mitigation processes to be employed, especially in the case of remote enrollments for which liveness assessment techniques are recommended to be deployed. We must consider that:

- In a semi-monitored process, detection observation should prevent photos or fingerprints from being used to match enrolled biometrics.

- In a fully self-service process, liveness detection must be employed with any biometrics matching function.
- While the most widely used liveness detection today is active liveness (the user must do something to verify their presence), passive liveness detection may be a better alternative.
- Comparing the biometric of the person to a mobile ID is good however certain risk policies will require the comparison of the person to the ID as well as to an offsite database (national ID database, etc.)
- Based on the risk associated with the transaction, biographical data may also need to be used and compared to an authoritative source as an added mitigation measure.
- The Facial biometric (photo) can be embedded in a chip, QR code, bar code, etc. and used as a component of establishing the validity of the document.
- Biometric matching processes may be employed to establish/confirm the binding of the document to the individual asserting the identity; matching references could include
  - Picture, fingerprint and biographical information
  - Data Cross-reference comparisons of data from the chip, bar code, and/or national/state database(s).

### **Data Protections and Privacy Controls**

The digital credential data must be cryptographically protected from manipulation or misuse, meaning that any tampering would be readily evident through inspection of the data elements.

In addition, privacy must be assured so that outside interests cannot access the information for fraudulent purposes. Encryption should be used on the chip or database that can be accessed to prevent misuse. Also, chips should be used to store sensitive data that can only be accessed by obtaining an “unlock code”. While some documents are not as sensitive as others, levels of security should be considered with differing requirements. For instance, logical access obtained through the use of an eID for a person's own information may not

*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.*

carry the same burdens as gaining access to other citizens' financial records. Where high security requirements need to be met, all biometric data should be in template form and depending on the sensitivity of the data, hashing might also be used to ensure data integrity.

The digital credential is meant to be the trust anchor for many digital transactions. As such, the process from enrolment to storage of the data and methods to ensure that the stored data is unmodified after personalization by the Issuer must be addressed by any offering.

## Life Cycle Process Support

### Process 1 – Unattended/Remote Vetting & Digital Identity Provisioning

Unattended/Remote Vetting addresses a scenario in which an end-user wants to remotely enroll in a program that requires the authentication of their identity. They want to use their mobile device to facilitate their identity proofing through the presentation and verification of “identity evidence” (such as an identity document along with their biometrics) in order to establish a digital identity credential. Digital Identity Provisioning is the process by which that digital identity credential is written to a secure container within the end-user's mobile device. The digital credential could then be used within that program with the same equivalency as the physical identity document, or any with any other program federated to accept that credential.

#### Identity Proofing to establish the Trust Anchor

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. In an unattended enrollment scenario, the verification of the identity of the requestor is paramount. Establishing a trusted Identity Anchor as the basis of the Digital Identity is

critical. For this reason, the individual requesting a credential must be able to follow a simple set of mobile device prompts to quickly and easily perform a very sophisticated process – one that is required to ensure the authenticity of the identity supporting the creation of the digital credential and to protect its use as it traverses the electronic ecosystem for which it is targeted.

#### Biometrics bind the Individual to the Trust Anchor

Whether the credential being provisioned to the device is meant to support travel (i.e., Digital Travel Credential (DTC)) by carrying a digital representation of the ePassport on the device; or to support driving privileges or age verification processes (i.e., Mobile Driving License (mDL)) by carrying a digital representation of the driver license on the device; or is meant to be used in place of a physical ID badge for access to certain facilities/areas, the root of trust for the digital credential must be strongly vetted at enrollment. Further, the digital credential must securely bind the biographic data of the individual asserting the identity to a verifiable biometric being held within the digital credential. Typically, cryptographic security mechanisms are used to bind the data and protect it from misuse. The specific biometrics selected, and the source of those biometrics, play a key role in the processes used to establish the digital credential, and form the basis of trust for authentication when the credential is used.

For both DTCs and mDLs, the biometrics are captured by the government issuer along with the biographic data submitted by the individual when they request the physical identity document (ePassport or driver license, respectively). That data can then be leveraged during the creation of the digital credential.

#### Digital Credential Delivery

Delivery of that digital credential will be Issuer-dependent, but in all cases, biometric authentication of the individual should be performed as part of the provisioning process to the device. A process that is being followed by several mDL Issuers involves the requestor using their mobile device to perform a

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

document authentication, facial recognition matching (FRM), and liveness process to confirm their identity prior to the mDL being sent to the device, as follows:

1. After the registration process is completed at the DMV, the requestor accesses a web portal from their mobile device to request that the mDL be loaded onto that device.
2. The portal application then prompts the requestor to take a picture of their current driver license and submit it to the portal.
3. The portal performs a document authentication process by assessing the document security features that are expected to be present on the document (varying by document classification and series), to ensure that an authentic document has been presented. In parallel, the DMV database is used to confirm the biographic data found on the image.
4. Once the document authenticity has been proven, the requestor is prompted to capture and submit a selfie image to an FRM process to confirm that the requestor is the person that was issued the physical document. Generally, this is a 1:1 comparison of the selfie to the image stored in the DMV database.
5. Typically, a liveness process is also invoked to ensure that the requestor is actually a live person rather than a picture of a person. The liveness check can be performed either before, after, or in parallel with the FRM process.
6. Once the identity verification has been completed successfully, then the mDL is made available for download to the requesting device.

The registration and delivery processes for DTCs can take several forms, based on the mechanisms allowed by the Issuing State. These processes may mirror the processes described for the mDL above and will be strictly tied to the authenticity of the physical ePassport as the trust anchor. Whether issued in parallel with the physical document, self-derived from the physical document, or issued in place of the physical document (i.e., as an emergency travel document),

the authenticity of the source/physical credential needs to be established at the beginning of the process, and the binding of the requestor to the authenticated document through Facial Recognition Matching (FRM) processes and liveness checking is imperative.

## **Process 2 – Biometric Capture and Authentication**

In this process, biometrics are captured by the Issuer as part of the original registration process; and subsequently confirmed through a self-service mobile capture and confirmation process as part of the delivery of the digital credential. To support remote identity vetting prior to credential delivery to the device, the biometric assessment of the device holder to an authenticated image (from the Issuer DB or from the securely stored image within the ePassport) must be performed.

It is important to note that the image that is printed on the front of either a driver license or an ePassport data page may be used as the comparison image, but often times these images are partially obscured by one or more of the physical security features protecting the document, so the use of a higher quality source image is recommended. Therefore, the image from the chip in the ePassport or the image held in the Issuing DMV database should be used as they provide the best quality source image for FRM processing.

### **Frictionless Capture**

As document and selfie capture on a mobile device are often difficult, measures should also be taken within the mobile device-based application to guide the requestor through the image capture and liveness processes, or to automate the capture of the images with as little end-user direct interaction as possible. For example, rather than ask the end-user to hold the camera over the document and press a button once they think they have the document properly in the camera window (and often times causing the image to go out of focus), a better practice is to allow the application to auto-capture the image while the end-user simply holds the camera in place over the document. The quality of these images directly affects the

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

success/failure of the authentication processing, so automation can not only increase the quality of the image captured but also reduce the friction to the end-user employing the application.

## **Identity Assurance**

When implemented correctly, the identity verification/proofing process:

1. establishes a root of trust/trust anchor on which to build a chain of trust linking the document authentication of the physical security features,
2. performs the passive authentication of the cryptographic security features,
3. performs the facial recognition matching of the image from the authenticated document to the individual presenting the document, and
4. provides the confirmation of liveness of that individual.

The cryptographic chain of trust ensures that the process was not compromised within or between any of the component steps and provides the auditable artifacts required to support the establishment of the digital identity that can assert the same level of identity assurance as the physical document. In terms of federal digital identity guidelines for Enrollment and Identity Proofing (see NIST SP 800-63), and the asserted identity assurance level of the digital identity, this process could be used to satisfy Identity Assurance Level 2 (IAL2) requirements related to remote vetting, where the “evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity”.

## **Process 3 – Store biometrics**

### **Image Quality Controls**

As a core concept of the transformation from the use of a physical document to its digital equivalent, the digital identity token will contain the facial image biometric from the source document (i.e., Data Group 2 of an ePassport) or its supporting source database (i.e., DMV repository). These images are high quality images that are well suited for FRM processing so that False Acceptance Rate/False Rejection Rate (FAR/FRR) considerations are negligible.

### **Data Protection 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. The facial biometric image, and the other biographic data from the physical document, need to be held within a Logical Data Structure (LDS) that is cryptographically protected from tampering and PII extraction without consent. The cryptographic protections on the LDS are well established for the data held within the electronic chip of an ePassport.

These protections are required to be kept intact as the DTC is generated and employed. As such, Passive Authentication (PA) must be used to authenticate the source document from which the digital credential is being derived; and PA must be performed against the LDS when the digital credential is extracted from its protected container for use in a relying party transaction. Throughout the duration of the transaction, the chain of trust for that transaction must be enforced to prevent data substitution or compromise. That is, a closed boundary must be enforced for each transaction.

### **Access Control Mechanisms**

Protection of and access to the derived digital credential is the next area to consider. These functions will be dependent on the protections available on the token or device hosting the credential. While protection of the digital credential itself is well established, access to the container hosting the derived digital credential must be carefully considered. Physical

*Sharing the biometrics from the digital credential with the relying party provides a basis for the verification of the individual performing the transaction.*

protections inherent in the device are a reasonable basis for protection of the digital identity object (i.e., DTC or mDL). It is recommended that the object be stored within the most secure area available on the device. This location is technology dependent and can range from the TPM chip of a laptop, to secure SIMM storage, to partitioning within a secure workspace or secure element of a mobile device.

### **Privacy by Design and Consent Mechanisms**

Regardless of the storage container selected, access to the digital credential must enforce authentication to the container as well as provide consent of the end-user for the release of specific elements from the digital credential. While fingerprint or facial biometric matching processes are employed by several device manufacturers, they do not necessarily ensure that the person accessing the digital credential is authorized to do so, so a separate authentication mechanism is recommended for access to the container.

One example of this may be the requirement to enter a PIN to open the application. Before releasing the data from the credential once it has been opened, a consent mechanism must be defined as well. This could be as simple as a checkbox being tapped by the user to acknowledge their consent for sharing the data specific to the type of transaction being performed. The data released would then only include those elements required to assert the attributes required by the transaction. This approach implements a privacy by design concept employed within a process consented to and authorized by the credential owner.

## **Process 4 – Share biometrics**

Sharing the biometrics from the digital credential with the relying party provides a basis for the verification of the individual performing the transaction. While workflows vary on the steps required to verify an identity in order to complete a transaction, FRM is well supported using the digital credential. Basically, that credential is shared with the relying party; the relying party performs Passive Authentication of the credential to ensure that it is intact, and then extracts the facial biometric to be used as the basis for an FRM process.

### **Self-contained versus Distributed Workflows**

The key to this process is controlling the interaction with the image capture device used by the end-user so that a chain of trust can be established between the relying party application and the external resource providing the comparison image. One way to ensure both the security and privacy of this external processing is to send a hyperlink via SMS to the mobile device of the end-user. This link can then be used by the end-user to initiate a selfie capture process that is run on the phone but transfers the data from the transaction back to the relying party. Additionally, IP/geolocation monitoring of the device might also be enforced for the transaction.

### **Trust Framework supports Secure Sharing of Biometrics**

In support of the many Seamless Traveler initiatives, this type of biometric sharing process allows the digital credential to be submitted to and authenticated at the beginning of the journey, resulting in the establishment of the traveler's facial biometric as the trust anchor from that point forward. Establishing that trust anchor within the travel continuum can be performed during check-in at home, in route to the airport, or as part of an airline counter interaction. From that point forward, FRM processes can be used to confirm the individual at bag check, for entry into an airport lounge, for tracking duty free purchases, boarding the plane, transiting the destination border, renting a car, and checking into the hotel – without the need for the traveler to produce a physical identity document.

## **Physical versus Digital**

The use of biometrics is important to the mitigation of risk associated with any transaction of value. A capability that reduces the friction inherent in any biometric process is key to user acceptance and use of the capability, but security and privacy controls must be properly implemented.

### **Data Privacy**

With physical identity documents, there is little control of the release of private information once the document has been presented. While there may be physical security features that can be evaluated to assess the authenticity of the document,

*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.*

not every relying party knows what to look for on every document that might be presented or uses an automated process for this assessment. Fewer yet use automation to match the image on the document to the face of the individual.

Digital credentials address all of these considerations since cryptographic mechanisms are employed to assess the authenticity of the credential, to protect the credential from tampering or data substitution attacks, to protect the privacy of the data, and to enforce consent mechanisms prior to release of any data from the credential. Further, FRM processes can be employed to match the facial image from the digital credential to the person performing the transaction with certainty.

### **Identity Authentication**

Presentation and assessment of a physical document is resource intensive and often not effective in establishing the identity of an individual or the privileges asserted by the document.

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. Automated processes can be orchestrated to provide an experience with less friction and higher satisfaction for the credential holder, and less risk for the relying party. Strong security, privacy, and consent controls can be included and enforced with this orchestration and provide value to both parties.

The binding of biometrics to the identity established within the digital credential allows that biometric to be readily used to prove one's identity without the need for a physical

document. Cryptographic protections of the digital credential prevent its misuse or alteration, bind the identity attributes to the individual, and support the automated assessment of the authenticity of the credential and its contents.

While physical documents have inherent value to support specific use cases, the value of properly implemented digital credential processes based on a biometric-bound trust anchor is seemingly unlimited.

## **Conclusion**

This white paper supports the transition from physical cards to secure mobile credentials in the context of leading-edge issuance programs for mobile Driving Licenses (mDLs) and Digital Travel Credentials (DTCs).

Physical credentials are used to assert everyday privileges, as well as to support the verification or confirmation of information about the credential holder and the permissions associated with the credential. Digital credentials provide an equivalent assertion of both identity and privilege as the source (physical) identity document from which it is derived. The incorporation of biometrics is required to establish the digital credential and bind the individual to the credential. This digital trust anchor can readily be authenticated against global trust frameworks by any relying party through automated processes. As such, the authenticated eID can be used to support age verification, car rental, border crossing, and access to secure and restricted facilities. These global identity authentication trust frameworks can be leveraged to support both provisioning and relying party processes. The exponential growth and supported capabilities in mobile devices make all this possible.

---

This document is an initiative of the IBIA Mobility working group and has been written by:

Magruder Dent  
Aware

Bill Dumont  
Innovatrics

Paul Townsend  
Acuant

Jean-Baptiste Milan  
HID Global

Tovah LaDier  
IBIA

**#identitymatters**



International  
**Biometrics+Identity**  
Association

1325 G Street, NW, Suite 500  
Washington, DC 20005

**202.888.0456 | IBIA.ORG**