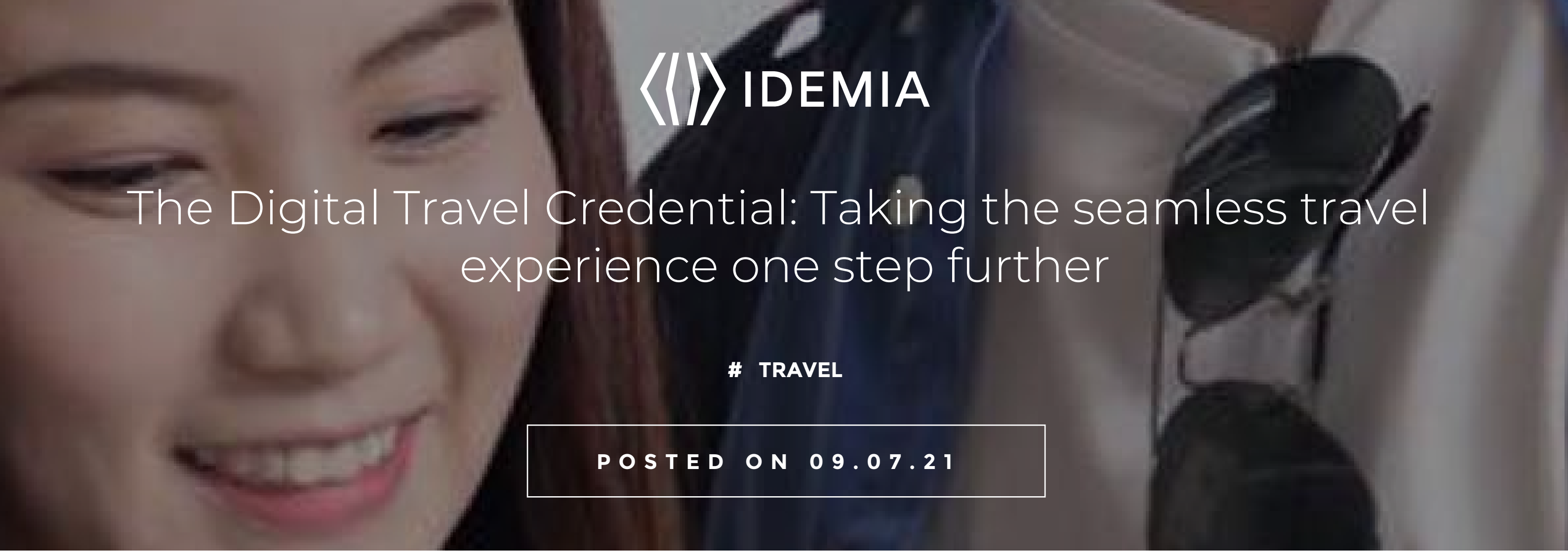


IDEMIA

The Digital Travel Credential: Taking the seamless travel experience one step further

# TRAVEL

POSTED ON 09.07.21

> *While domestic and international restrictions imposed to combat the spread of the COVID-19 virus have a tremendous impact on cross-border passenger volumes, and the longer-term picture remains unclear, it is no less important to continue to leverage the latest technologies to both strengthen borders and improve traveler experiences. Over recent years, the technology has radically evolved in fields such as identity, security, biometrics and mobile applications to do exactly this. Technology has already transformed the world of border security and efficient processing of passengers, for example through secure ePassports (also known as an electronic Machine Readable Travel Documents or eMRTD), automated eGates, biometrics used to assure visa regimes, and mobile boarding passes. However, the story is far from complete. A newer generation of secure and efficient solutions are just beginning with the development of the Digital Travel Credential (DTC).*
>
> Secure Identity Alliance, July 2020

Bringing ePassports into the digital era

The travel industry has been continuously innovating to maintain safe and smooth travel in the face of complex challenges. Innovations like automated self-service kiosks are deterrents of fraudulent activity while enabling travelers to identify and authenticate themselves using their **biometric data**. Digitalization has not only sped up the border control process, but it has also increased the efficiency of border management systems at land, air and seaports.

Despite the tremendous **technological advancements to various aspects of the travel process**, there is an integral part of worldwide travel that has not evolved at the same rate, the passport. The level of trust and confidence in the passport means that although there is great enthusiasm to digitalize this document, there is no overestimating how great an undertaking it is. **The digital passport must at least deliver the same standard of security, reliability and privacy as the current ePassport** in order to maintain global trust and interoperability.

Governments are now exploring ways to digitalize the passport so that passengers can continue to enjoy a seamless travel experience. To achieve this the International Civil Aviation Organization (ICAO) and International Organization for Standardization (ISO) are working with governments and technology experts to define and develop the technical specifications for the Digital Travel Credential (DTC).

> *There is little doubt DTC will be at the center of a new generation of border management systems that increase security while speeding the passenger journey through airports and*

> *across borders.*
>
> Secure Identity Alliance, July 2020

Main principles of the Digital Travel Credential

The Digital Travel Credential is a **virtual credential** derived from a state-issued document. It is an exact representation of the electronic machine-readable travel document (eMRTD), that includes the holder's facial image, biographical data, and security features. Based on secure Public Key Infrastructure (PKI) technologies, the DTC is securely stored on the holder's device, and can only be shared with the holder's consent.

As expected, the implementation and deployment of the Digital Travel Credential relies on the expertise of technology providers. In order to ensure global interoperability, all providers must be fully compliant with the technical **specifications defined by ICAO and ISO**.

> *With respect to authenticity and integrity, the DTC MUST be at least as secure as an eMRTD*
>
> ICAO

Currently, passports are used as an authentication factor for proof of possession, identity and nationality. Due to the **reliability of passports** their use has expanded beyond the travel industry. With the holder's biographic and biometric data stored on a chip, the ePassport is relied upon in a variety of use cases where absolute confidence in a person's identity is required.

For the Digital Travel Credential to be globally accepted it must fulfill these uses and provide at least the same level of security and interoperability.

A hybrid approach is being used to develop the DTC, comprising of two elements that are linked cryptographically:

- **A virtual component (VC):** A transportable data file which contains a copy of the biographic and biometric data in the physical passport.
- **A physical component (PC):** This is currently the physical travel document itself, however it could be replaced by a secure element in a smartphone for a fully paperless experience.

There are three types of DTC:

	Self-derived DTC Type 1	**Authority derived** DTC Type 2	**Authority issued** DTC Type 3
Issuance Once and for all	Generated by holder Holder scans the passport	In person – generated by state Holder presents the passport	In person – issued by state No passport
Usage for identification at border control	Passport is required	Passport is for reference purposes only	Smartphone only

In November 2020, the first DTC – self-derived – was endorsed by the ICAO. To date it is the only one that has been specified and approved by the organization. Specifications regarding the physical component defined in Type 2 and 3 are expected in 2022.

Passport booklet and smartphone	**Self-derived** DTC Type 1	**Authority derived** DTC Type 2	**Authority issued** DTC Type 3
Description	The DTC on the mobile device is a representation of the same data that can be found on the chip of the passport.	The DTC on the mobile device is equivalent to the physical passport.	The DTC on the mobile device is the only source of traveler information, with no reference to a physical document. This third level is relevant for a temporary emergency travel document.
Status of ICAO standardization	Technical specifications: certified in September 2020	Technical specifications: certification expected in 2022	Technical specifications: certification expected after 2022
Physical component	**eMRTD**	**Mobile device and eMRTD** (passport for reference purposes only)	**Mobile device, temporary emergency documents**
Virtual component	**Mobile device/cloud**	**Mobile device/cloud**	**Mobile device/cloud**
Relationship between the physical and the virtual component	The physical component is the passport. The virtual component is composed of the data contained in the chip (Data groups 1 and 2).	Cryptographic link between the physical component, the smartphone (the physical component), and the virtual component, composed of the data contained in the chip.	Cryptographic link between the physical component, the smartphone (the physical component) and the virtual component, issued by the passport authority. The passport is no longer used.

DTC enrollment and issuance processes	**Remote** Anytime, anywhere. Biometric enrollment and Presentation Attack Detection (PAD) are recommended to prevent identity fraud and increase trust in the DTC.	**In-person** Face-to-face process. Supervision by a member of the city hall is advised. Biometric enrollment is recommended for a fully paperless journey.	**Remote** The traveler receives the DTC directly from the travel document issuing authority. Biometric enrollment and PAD are required to prevent identity fraud and to increase the level of security.
DTC uses	Depending on the journey, the traveler will be able to go through touchpoints by simply using their smartphone and biometrics. However, they must show their passport at least once, for example, at border control.	The traveler uses only their smartphone or biometrics to prove their identity through all touchpoints.	For emergency documents, the traveler may only need to present their smartphone or biometrics to prove their identity.

The digitalization challenge: creating a secure and reliable Digital Travel Credential

One of the major objectives of the DTC is to ensure a level of security that is equivalent to the physical ePassport. Bearing in mind that passports currently provide verification of the holder's entitlement to state benefits, it is imperative that when it is replaced by the DTC, the confidence and security of both the holder and state are maintained. This requires a reliable process for the acquisition of personal data, especially biometric data, including face, fingerprints and/or iris.

Step 1: Creating the virtual component

Users are able to create their DTC from the comfort of their home using the national **mobile ID application** via their personal device. As this is an unsupervised process where the user is remote, it is vital that the user's identity is verified as part of the DTC creation. To achieve this, the mobile ID application has access to national databases ensuring that the process is secure, and the data is reliable. The application will perform:

Automatic passport scans and authenticity checks:

To start the issuance process, the mobile ID app will ask the user to scan the data page of their ePassport, specifically the MRZ. This extracts the user's information and photo from the chip. Before reading the data, the app will verify the data in the passport to check it has not been modified, and that it has been signed by the government.

- **User identity verification:**

To authenticate the identity of the passport holder and ensure they are the legitimate owner, the national ID app will perform:

- **automatic live face capture and PAD**. For a user-friendly experience, passive detection systems are recommended.
- **biometric verification** – the national ID app will compare the live selfie to the photo extracted from the passport (1:1 biometric matching).
- **knowledge-based verification** by accessing non-public data. The national ID app will cross check the user's information with this "hidden" data to confirm their identity.
- **Authentication factors:**

To finalize the virtual component issuance process, the national ID app will ask the user to define up to three authentication factors:

- **Biometric data**: who the holder is
- **Smartphone**: what device the holder is using
- **PIN code**: information only the holder knows

Once the virtual component of the Digital Travel Credential has been created, the user can stop the digitalization process here, i.e. type 1. When the user is traveling, **their passport will need to be presented at least once during border clearance**. However, if the user wants to enjoy a completely paperless travel experience, they can link the virtual component of the DTC to their physical component (type 2) during a face-to-face appointment at the local city hall.

Step 2: Linking the virtual and physical components

Similar to the data page of the current ePassport, the virtual component contains information that must be shared in order to verify the holder's identity. This information ensures compliance with existing verification rules for passport use. The link to a physical component allows authorities to check that:

- the DTC has been issued by an authorized entity.
- the data on the virtual component has not been altered.
- the DTC has not been cloned through an authentication process similar to the current eMRTD.

The linking process will be supervised at a municipality, and will be based on the eMRTD. Alphanumeric checks and biometric authentication will precede the mandatory authorization and key delivering performed by the state issuance authority. This **cryptographic link** will reuse mechanisms already defined by ICAO. For example, the ones already established in current eMRTDs, such as chip authentication, active authentication, anti-cloning, etc.

Additionally, the face-to-face issuance of the physical component will provide the opportunity to **expand the features and uses of the DTC**, for example:

- Storing additional data during the issuance process, i.e. a high-resolution ICAO portrait, which has been signed by the issuing authority during a supervised process.
- Storing the DTC on a different device.
- Considering the current health crisis, it may be useful to develop a secure link between the DTC and the Health Travel Pass to verify the holder's health status and fitness to travel.

Step 3: Securing the Digital Travel Credential

Only the issuing state will have the capacity to authorize and certify the creation of a link between the virtual and physical components of a DTC. A **PKI cryptographic technology** will protect the encoded data. Additionally, the verification of the digital signature, provided by a Single Country Signing Certification Authority (CSCA), will give border authorities assurance of the authenticity of the DTC.

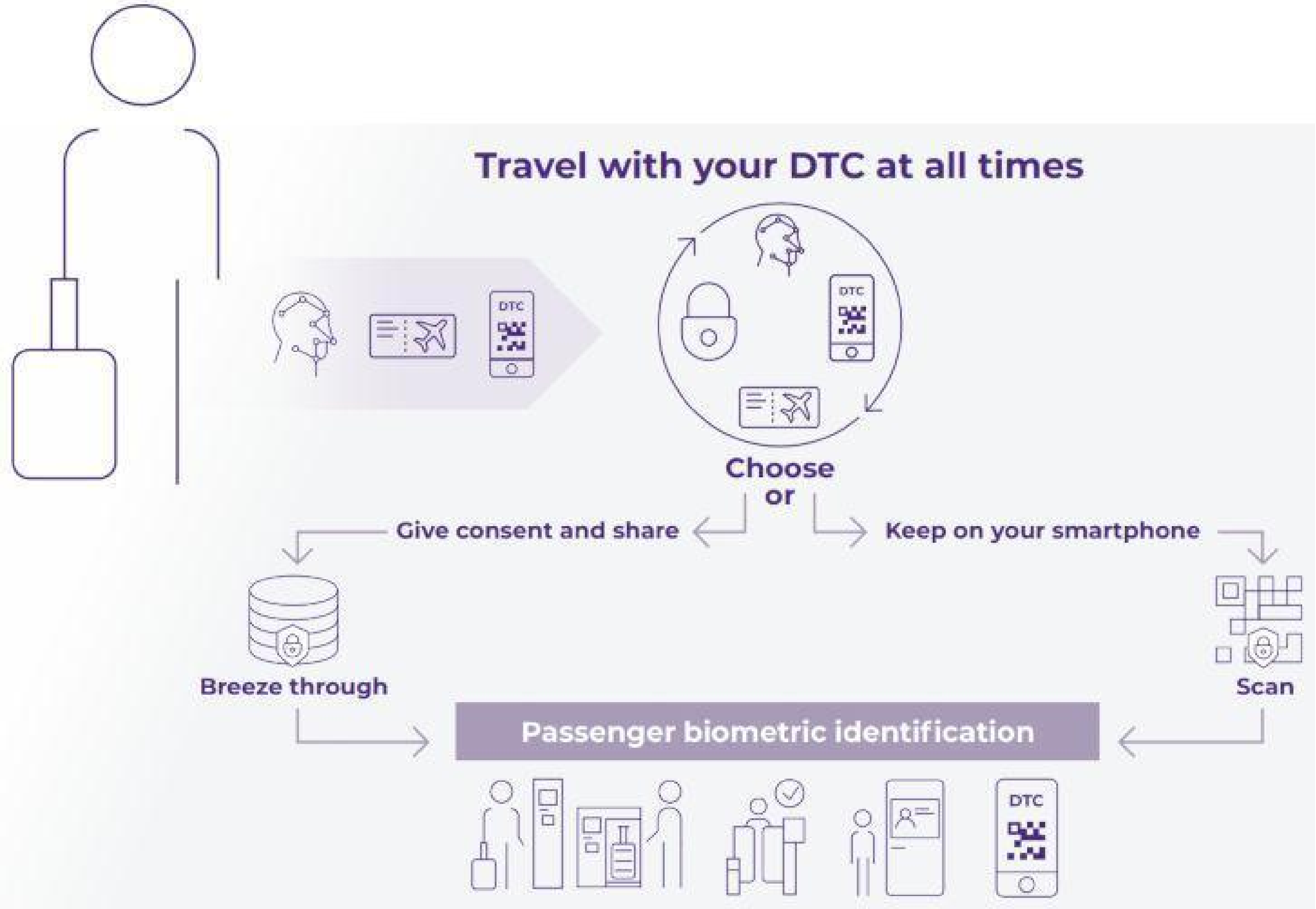
The Digital Travel Credential in action: exploring new opportunities

The DTC will allow border agencies, port operators and carriers to improve their efficiency while providing a safe and smooth travel experience.

Ease of use and contactless interactions are two of the main benefits of the DTC.

A unique identifier for a safer and more convenient travel experience

Thanks to their Digital Travel Credential, travelers will be able to prove their identity throughout their journey without providing a passport. From the comfort of their home, the holder can use a check-in app to consent to having a temporary unique identifier created. The app will then **combine their biometric data, DTC and travel information** to create the unique identifier which can be used to verify their identity at multiple touchpoints throughout their journey. This synergy between security and convenience means that efficiency in passenger flow is greatly improved at border crossings. The touchless design of the DTC and the fact that it is stored on the user's device are critical mitigating factors in terms of **hygiene concerns**. The user only touches their own device. In light of the current public health crisis, **contactless capabilities** are key to reassuring individuals that it is safe to travel again.



The general increase in digitalization across various industries means that individuals have become accustomed to providing their personal data. They understand that in order to receive a more personalized service and, in terms of travel, to gain access to accurate and up-to-date information they must consent to the capture of their personal data, including biometrics. However, despite this familiar trend, there is one concern that will need to be robustly addressed so that traveler trust is maintained. That concern is **data privacy**, i.e. understanding who will have access to the holder's personal data.

To remove the uncertainties around unauthorized access to private data, users will have the opportunity to choose between two options:

- **Store their unique identifier in their smartphone**. In this case, they will have to scan their smartphone at every touchpoint to verify their identity.
- **Temporarily give consent to share their unique identifier** with a central database. In this case they will be identified using their biometrics at multiple touchpoints

In both cases, consent is mandatory, which gives the user control of their personal data at all times.

Governments and port operators will optimize their border clearance process

The Digital Travel Credential will help government agencies to perform the necessary traveler checks prior to their arrival. This allows officials to be fully informed of who will be arriving, enabling them to welcome bona fide travelers, and take appropriate measures against individuals who pose a threat. Indeed, the automatic retrieval of travelers' data and pre-arrival processes such as **electronic travel authorization** and on-the-spot visa issuance, will benefit from better data quality, and a decrease in errors and cases of intentional data manipulation.

The digitalization of the travel document will also provide government agencies with better travel history, allowing them to **detect suspicious patterns and anticipate risks**. As soon as a travelers share their DTC, government agencies can process or cross-check travelers' data against reference databases and analyze it via a **risk assessment solution** in order to ascertain security clearance.

In the context of a sanitary crisis, government agencies and port operators may ask for additional checks in order to permit cross-border travel. Travelers may need to declare or prove that they are healthy, and a convenient and trustworthy option is to **link the DTC to a 'health passport'**. It may also be necessary to know if a traveler has flown from, or transited in, a 'high-risk' area before arriving at their final destination, or if they were close to infected passengers on a plane. It is needless to say, an **appropriate balance between security and privacy** will have to be actively maintained.

Carriers will be able to benefit from improved information accuracy at check in

Carriers will have fewer errors concerning traveler information during check in. The Digital Travel Credential will guarantee data integrity as it is derived directly from the national ID app and transmitted as soon as the traveler grants consent to share their DTC. This will significantly improve the data quality.

Thanks to DTC and biometric data, carriers can securely move the entire check-in process online. This will allow them to anticipate travelers' arrival at the airport and thus allow better management of the flow of travelers and reduce waiting time.

A seamless travel experience: from theory to reality

Standards and specifications are necessary to provide guidance on how the Digital Travel Credential should be generated, however the overall success of the DTC relies on its adoption by all of the entities that are part of the traveler's journey.

The main priorities include ensuring ease of implementation and a user-friendly experience. Governments have the responsibility of deciding on an approach that will produce the best outcome for their travel ecosystem.

> *Of course, developing a credential that will be embraced by governments, industry and citizens, and accepted throughout the world, is an inherently complex undertaking that takes time. But, with work continuing at pace, it won't be long before vision becomes reality. With the recent coronavirus experience, travel documents might need to incorporate health certificates and this must be kept in mind in the development of the DTC.*
>
> Secure Identity Alliance, July 2020