POSITION PAPER

The Digital Travel Credential

Taking seamless travel one step further by simplifying the travel process while increasing security and privacy

IDEMIA

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 traveller 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 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

IDEMIA

Bringing passports 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 biometrics.

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 sea ports.

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 deliver at least the same standard of security, reliability and privacy as the current passport 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).

Key facts

June 2017
The ICAO NTWG*

established a specialised subgroup and tasked ISO* with standardising travel credentials

- DTC must be issued by a Travel Document Issuing Authotity
- DTC must be as secure as an eMRTD

Nov. 2020
the DTC type 1 was endorsed by the ICAO

“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

NTWG: New Technologies Working Group
ISO: the International Organization for Standardization

Main principles

The DTC 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 DTC 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.

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 information stored on a chip, the passport is relied upon in a variety of use cases where absolute confidence in a person's identity is required.

For the DTC to be globally accepted it must fulfill the same uses as the physical passport, 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:

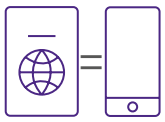
A virtual component (VC)

› A transportable data file which contains a copy of the biographic and biometric information in the physical passport.

A physical component (PC)

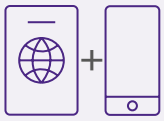
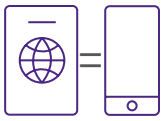
› This is currently the physical travel document itself, however it could be replaced by a secure element in a smartphone for a fully paperless experience.

There are three types of DTC:

	> DTC Type One Self-derived	> DTC Type Two Authority derived	> DTC Type Three Authority issued
	DTC Type 1 	DTC Type 2 	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.

IDEMIA's approach to the three types of DTC

	DTC Type 1	DTC Type 2	DTC Type 3
Passport booklet and smartphone			
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 temporary emergency travel documents.
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, and the virtual component, composed of the data contained in the chip.	Cryptographic link between the physical component, the smartphone, 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.

Creating a secure and reliable DTC

One of the major objectives of the DTC is to ensure a level of security that is equivalent to the physical passport.

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 passport, 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:

- Biometrics: who the holder is
- Smartphone: what device the holder is using
- PIN code: information only the holder knows

Once the virtual component of the DTC 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 VC 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 VC has not been altered.
- the DTC has not been cloned through an authentication process similar to the current eMRTD.

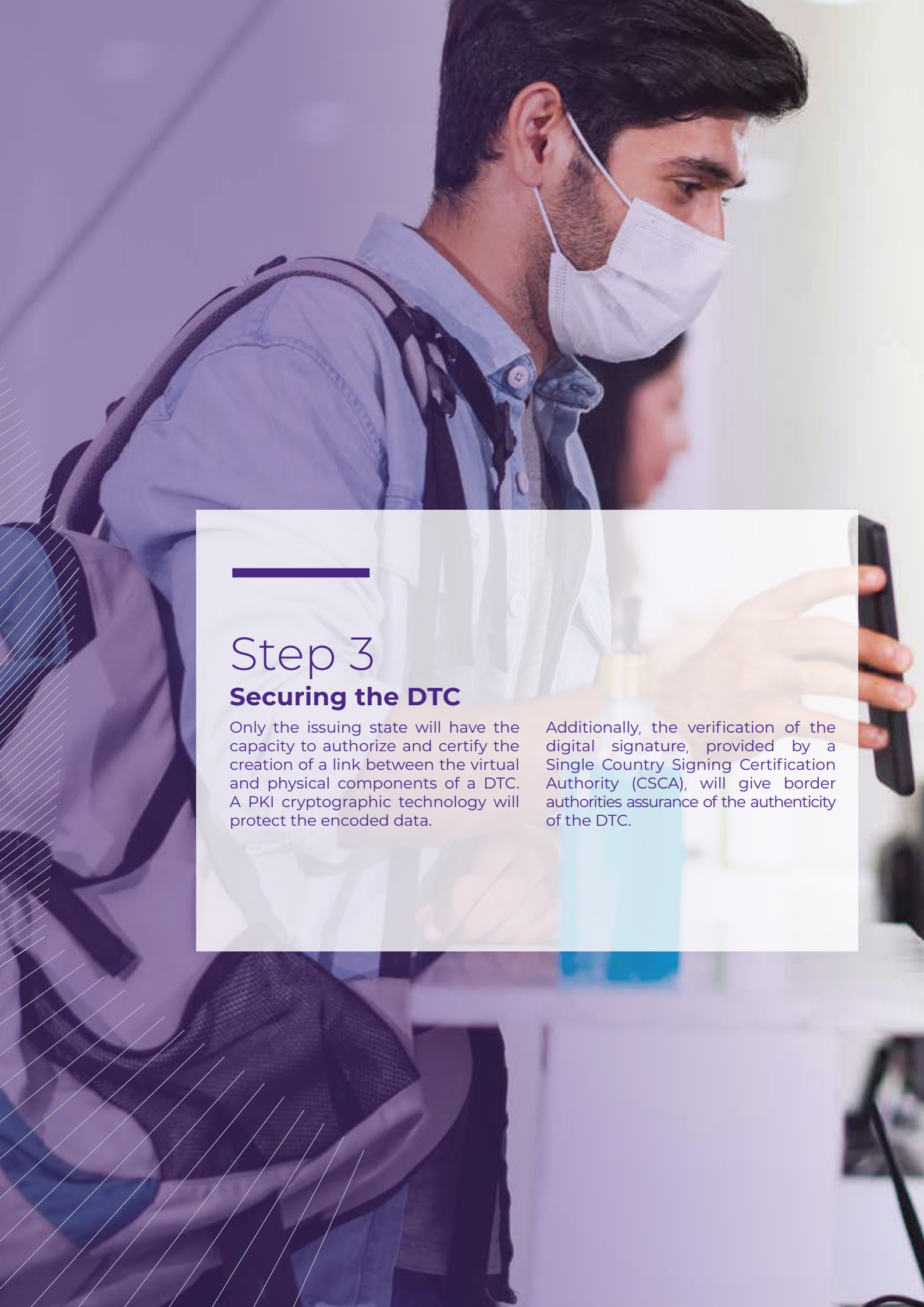
The linking process will be supervised at a municipality, and will be based on the eMRTD. Alphanumeric checks and biometric authentication will precede the mandatory authorization and key delivering performed by the state issuance authority. This cryptographic link will reuse mechanisms already defined 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.

"With respect to authenticity and integrity, the DTC MUST be at least as secure as an eMRTD."

ICAO, Oct 2020



Step 3

Securing the DTC

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.

DTC 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.

Passengers will experience a safer and more convenient travel experience

Thanks to DTC, 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 biometrics, 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.

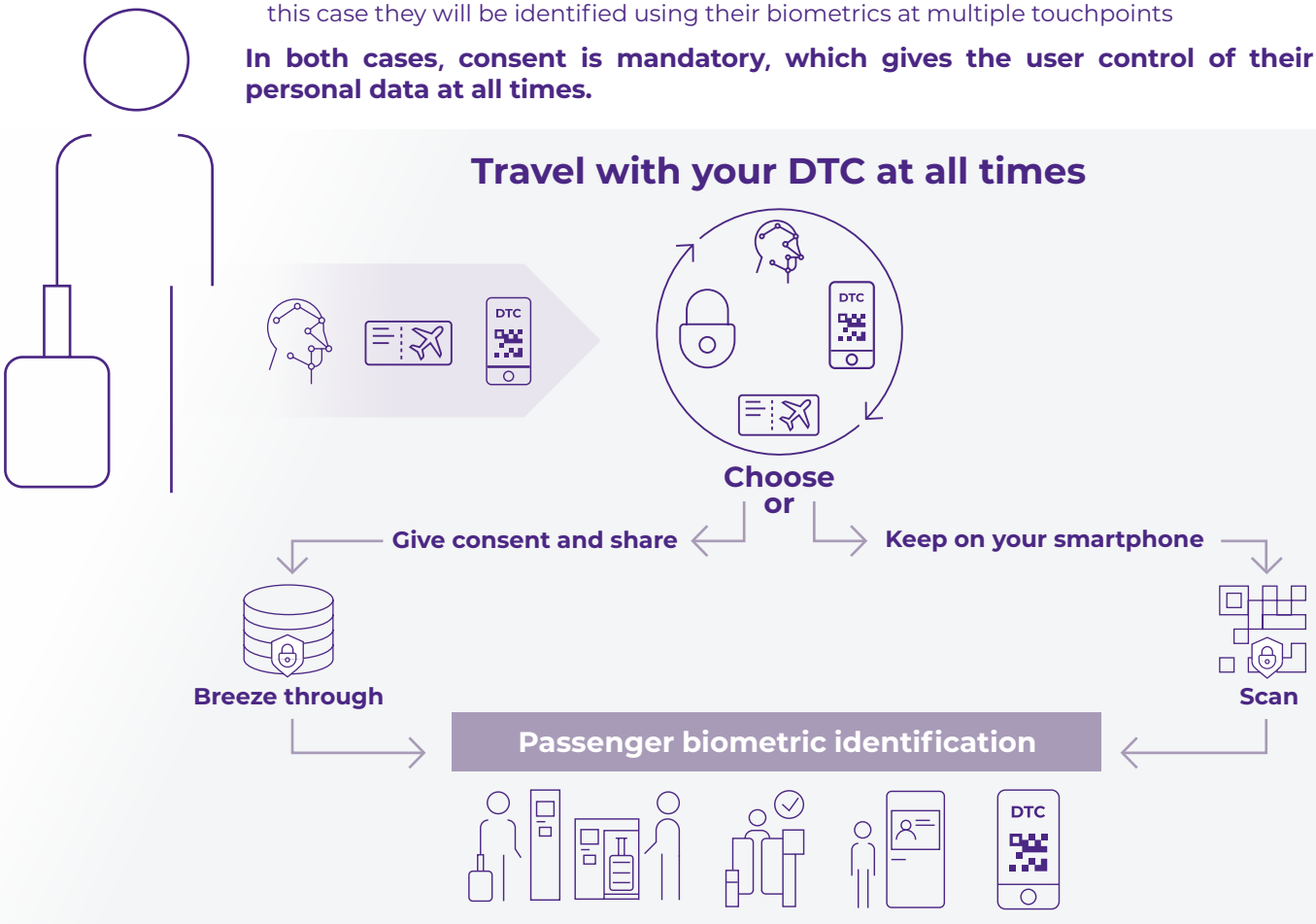
Passenger data privacy

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:

- To store their unique identifier in their smartphone. In this case, they will have to scan their smartphone at every touchpoint to verify their identity.
  or
- To 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 DTC 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 DTC will also equip 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.

"The DTC, sent in advance of the traveler arriving at the border enables authorities to conduct scenario-based targeting, watchlist lookup, etc."

ICAO Oct 2020

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 DTC 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 biometrics, 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.

From theory to reality

Standards and specifications are necessary to provide guidance on how the DTC 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.

IDEMIA, the global leader in augmented identity and security solutions, has the necessary expertise to help carriers, port operators and governments with their digital transformation to facilitate international travel. IDEMIA is currently working with ICAO to develop an agreed definition of DTC standards to guarantee its interoperability, and has developed a strategy for implementing it into existing solutions.

"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

IDEMIA

Interview with IDEMIA's DTC experts: Joost Van Prooijen and Jouri de Vos

What is your background and how would you describe your career path?

Joost

I have been in the identity business for 14 years. I currently work as a Manager of Innovation for IDEMIA Public Security and Identity (PSI) in The Netherlands. There, I lead a team of experts in the field of traveler identification management. I started my career at the Dutch Ministry of the Interior—the National Office for Identity Data (NOID). In collaboration with NOID, I worked on the foundational development of a biometric virtual identity document (vID) that enables traveler identification, mobile in-person identification and online authentication. I have also been involved in working groups that prepare the Dutch implementation of the eIDAS trust framework for electronic identification.

Jouri

I have been working in the identity business for over 12 ½ years. I started off as an engineer where I worked on the certification of passport related chip projects in collaboration with the Dutch government. A large part of my career path has been centered around working on identity projects in the Netherlands such as the implementation of the EU Biometric Passport and National ID Cards for Dutch citizens. I currently work as a Solution Designer and Technical Consultant for IDEMIA PSI in the Netherlands, where I develop new innovative identity solutions. Over the past five years, I have been developing and researching digital identity projects in cooperation with NOID.

What do you do as members of the International Civil Aviation Organization (ICAO) working groups and workshops for DTC standardization?

Joost

I've been involved with ICAO since 2020 and I will be taking on a new role as a convener between ICAO and the International Organization for Standardization (ISO). This position is centered on bridging the gap between governments and the industry. For this role, I will be participating in working group three, where the focus is on developing the standards of passports and their digital versions (DTC).

Jouri

I have been involved with ICAO since 2019. I am a member of task force five, which is in working group three. This is where the creating and writing of the technical specification for DTC takes place.

What do you think are the main competences needed to issue a DTC?

Joost

Instilling and building trust are key when it comes to issuing a DTC. The DTC needs to be trusted by governments and issuing authorities because governmental data is being used.

Jouri

The information used for the DTC is from a passport and this information comes from issuing authorities. Our goal is to make a DTC as secure as the physical passport currently is. In order to create this trust, an issuing authority needs to have a role in the process of creating such a DTC. Another thing that is key is competence in regards to how we store this information.

Where do we stand today and where are we going?

Joost

We have a specification for DTC type 1, which is bound to a passport chip. As we're moving toward type 2 and 3, we need to define the technical specification of the DTC physical component so a traveler can use a phone or another device instead of a passport. We are looking at existing standards to help define the framework of the physical components. The idea is that in the future we can use either a passport or a phone to travel.

Jouri

Today, we currently have a digital copy of your passport. This is a DTC and it contains passport data and it can be shared. In the future, we would like to have an app that replaces your passport.

The Digital Travel Credential

Taking seamless travel one step further

idemia.com/**id2travel**

IDEMIA

Join us on

www.idemia.com