ENABLING SAFE, SECURE AND SEAMLESS TRAVEL TO ACCELERATE BORDER CONTROLS

WHY GOVERNMENTS SHOULD ADOPT DIGITAL TRAVEL CREDENTIALS

Enabling safe, secure and seamless travel to accelerate border controls

Building trust in the digital age

Despite significant advances throughout travel and tourism, many aspects of international travel remain encumbered by manual processes that are susceptible to fraud. For many years, aspiring voices from government and industry have advocated a vision of better travel experiences. A vision where outdated paper-based processes are replaced by modern digital processes that include strong identity assurance; and where passengers can travel from anywhere to anywhere using just their Digital Identity[1]. But as both the travel and tourism sectors – and the technology that underpins them – have been transformed, it is important for governments to begin developing their own strategies to deliver safe, secure and seamless travel for all international travelers, regardless of their mode of transport.

It is our firm view that this journey begins with "**trust**". And that trust can only be established by having absolute certainty a person is genuinely who they claim to be. Society in general and travelers, in particular, have come to rely on – and trust – digital processes in all other aspects of their work, life and travel. Once established, that level of trust will be easily verifiable and will enable the adoption of digital processes, faster operations, increased automation, costsavings across the industry, and the shortest possible route to accelerating border controls, improving operations and offering truly seamless travel experiences.

In this paper, we examine **Digital Travel Credentials** – what they are, what they can do, and why governments should adopt them.

What is a digital travel credential?

The global body responsible for passport standards, the UN's International Civil Aviation Organization (ICAO), has developed a standard[2] for Digital Travel Credentials that is built on the latest standards for issuing passports (i.e. ICAO 9303[3]).

The ICAO Digital Travel Credential, or DTC, is the authoritative standard for an international digital identity credential, designed for global interoperability. Other formats and modes, with similar properties and functionalities to ICAO's DTC, do exist and are in various stages of development and deployment. However, these are proprietary (i.e. nonstandard) and are exceptionally limited in terms of their usefulness, particularly when it comes to interoperability. For the sake of clarity, we refer to these non-standard variations as "Digital Identity Tokens". This paper weighs the pros and cons of different approaches to modern identity credentials, recognizing that some will work better than others to deliver the outcomes that are most important to governments at this time.

A DTC is simply a digital representation of a person's identity, typically derived from a physical identity document such as a passport. But the real challenge lies in understanding how to trust the authenticity of the digital data in the same way we trust the authenticity of the physical document. And this is made more challenging as the document – and the person to whom it was issued – might not be physically present at the time it is verified. That means the digital data, the DTC, must be secure and invulnerable to tampering or forgery.

Aleksei Markachev
Senior Product Manager, SITA

[1] For more on Digital Travel, download a copy of SITA's 2021 whitepaper here: https://www.sita.aero/resources/White-papers/powering-economicrecovery-restarting-travel-and-tourism/
[2] Ref. ICAO Guiding Core Principles for the Development of a Digital Travel Credential (DTC) https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx
[3] Ref. ICAO Machine Readable Travel Documents (MRTDs) https://www.icao.int/publications/pages/publication.aspx?docnum=9303

Confirming the document is authentic, belongs to the person presenting it, and ensuring their identity has been verified by enhanced techniques such as 'liveness detection', are all essential to the integrity of the process. And it must also be possible to authenticate the data and verify its accuracy and completeness. Not an easy task at the best of times.

Yet there is a well-established example of issuing digital credentials which serves as a powerful and timely reminder of how governments have learned to trust digital processes at the border: Electronic Travel Authorizations (ETAs[4]). With SITA's help, the Australian government introduced the word's first ETA system back in 1996. While there are of course some key differences between a DTC and an ETA, it is nonetheless important to recognize how each authorization is digitally linked to the traveler's passport, enabling airline check-in staff, among others, to confirm if the traveler has the authorization to board a flight to Australia. In the 25 years since, many other governments have followed suit by establishing ETA systems as the simplest form of visa, granting authorizations for travel to their country and building further confidence in digital processes at the border.

There are conversations to be taken forward regarding how digital data, specifically Digital Travel Credentials, are best shared with and used by government authorities and other stakeholders involved in a traveler's journey. But it is important to highlight how the technologies available today are already capable of delivering the next generation of digital travel capability. The technology exists and is being successfully used by a number of governments. The critical question today is: how to use it to deliver the best possible outcomes?

There is also a compelling argument to develop a global shared trust model to enable stakeholders, including government authorities and travel and tourism providers, to collaborate in real-time. But instead of waiting until such a global traveler data exchange platform exists, digital data can and should be verifiable locally – i.e. the entity verifying the data does not need to receive any confirmation from the entity who issued the Digital Travel Credential in the first place.

[4] Note: ICAO has published DTA specifications and guidance material as a companion to ICAO Doc 9303 Part 7

Challenges with paper documents

Physical travel documents such as passports have served us well for centuries. But as much of our life and work has come to rely more on digital and less on paper, the outdated process of verifying someone's identity still relies on a patchwork of manual and technical processes that require the passenger – and their travel document – to be physically present, whether at check-in or bag-drop, at a self-service kiosk or gate, or standing behind the counter waiting to be interviewed by a border officer. It requires specialized training, resources and experience to identify a counterfeit or forged travel document. And matching an old photo with the physical attributes of the person presenting it is fraught with potential errors and mismatches.

Additionally, key business processes, such as applying for an electronic visa (including ETA, ESTA etc.), already exist today and invariably mean that neither the traveler nor their travel document were physically present so their identity cannot be reliably verified. This places additional strain on the border, requiring officers to verify the visa holder's identity upon arrival, when the constraints of time, space and resources are under the most pressure.

Today, when a physical passport is presented as a credential, it is considered trusted if the document reader can verify the data on the chip as authentic; and the document holder (i.e. the person to whom the document was originally issued) matches the biometric data contained on the chip. However, this process involves queuing at a kiosk, gate or counter, and takes time to complete even when performed by an experienced officer using an automated document reader. The time needed to perform this verification only increases for infrequent travelers using unfamiliar systems and document readers such as those found in Automated Border Control (ABC) gates and kiosks. And it's important to highlight just how many times a passenger currently needs to present their physical travel document throughout their journey.

Bring on trusted digital travel credentials

With the advent of smartphones and mobile wallets, most mobile devices available today include a communication technology known as Near Field Communication (NFC). This is what enables us to tap our credit cards without needing to enter our PIN and use our phones as a digital equivalent of cash.

Thanks to NFC, travelers can now read their passport chip themselves, create a Digital Identity Token and store it on their device. However, up until now, this has also resulted in proprietary versions of digital identity data being stored inside various travel apps, meaning that the identity data only works for that particular app, greatly limiting its usefulness. Some applications store the Digital Identity Token in a secure wallet, outside of the specific app. But the non-standard nature of the Digital Identity Token limits widespread interoperability with all other stakeholders. All of this results in digital identities with a low level of trust that is difficult, potentially impossible, to share to improve border operations and enable the seamless traveler journey. While there are positive use cases of proprietary Digital Identity Tokens being used in airport processes, this is not yet the case for government authorities who would be unwilling to trust such a Digital Identity Token (or similar) to cross their border.

Ideally, a traveler will be issued a trusted, ICAO-compliant Digital Travel Credential (DTC) which can be sent to all concerned stakeholders in advance of travel. In the case of a border crossing, this would mean the border agency could perform their risk assessment, based on additional context data (including PNR, API and government databases for background checks etc.), and pre-clear the traveler well in advance of their arrival at the border – provided, of course, their identity is verified and matches the credential presented.

When combined with advance passenger processing (APP) or interactive advance passenger information (IAPI), the DTC can ensure that only those travelers who are currently authorized to arrive in the country can board the flight.

Then, when the passenger arrives at the border, they only need to present their face to be recognized as pre-cleared to enter the country. No need to present a paper passport, or even a mobile phone-based token, for inspection or to be read by a gate or kiosk.

When combined with Advance Passenger Processing (APP) or Interactive Advance Passenger Information (iAPI), the DTC can ensure that only those travelers who are currently authorized to arrive in the country can board the flight. And the addition of trusted identity and biometric data makes the government's risk assessment even more rigorous.

Making the case for the adoption and issuance of digital travel credentials

The Digital Travel Credential (DTC) is a vital enabler of Digital Travel. In a near-term future, travelers will be able to perform a myriad of important transactions using digital processes – from requesting a visa, to booking a flight, checking-in, arranging accommodation and, ultimately, crossing borders. With standards compliant, trusted DTCs, travelers will be able to share their verified identities in advance of travel, be recognized automatically when arriving at the border, and benefit from an accelerated border crossing process which will reduce pressure on resources, eliminate queues and eradicate wait times. Unfortunately, for those governments who delay their plans to issue DTCs, the opposite will be true: pressure on border resources will be greater, and queues and wait times will increase.

In anticipation of governments issuing Digital Travel Credentials (DTCs) as a standard practice when issuing passports to their citizens, travelers will be able to create DTCs themselves. This will involve scanning the picture page of their passport, positioning the chip next to the phone, and then taking a 'selfie' to verify against the photo stored on the passport's chip.

To avoid interoperability problems, such as those caused by attempting to work with multiple different types of digital credentials, we recommend governments examine how best to issue a standardized DTC directly to passport holders. When physical travel documents are issued, these could be accompanied by instructions for the traveler to visit a government-hosted, secure website to download their DTC. Passport holders can then store it in a secure digital wallet to be accessible to any application that needs to verify their identity. To ensure interoperability and security, governments can issue ICAO-compliant DTCs in a similar way to how they issue ICAO-compliant passports. And, as is already the case with outsourcing the production of secure travel documents, the DTC issuance process could also be outsourced to competent, trusted private sector organizations.

Enabling a safe, secure and seamless travel experience

Only when we have secure, verifiable Digital Travel Credentials that can be easily verified and sent to any stakeholder in advance of travel, will we be able to realize the promise of improved border operations and safe, secure and seamless traveler journeys. These credentials must be widely accessible to countless systems and stakeholders – and reusable for multiple travel-related processes across a range of journeys in all modes of transport for both domestic and international travel. Doing so will signal a clear commitment to embrace Digital Travel and reduce the industry's dependence on physical identity documents and manual processes.

It is worth examining what lessons can be learned from existing Electronic Travel Authorization (ETA) deployments – and the technical specifications ICAO, ISO, IEC and others are developing for Digital Travel Authorizations (DTAs[5]) – to better understand the optimum pathway to issue Digital Travel Credentials (DTCs). We would strongly recommend governments start making plans to issue ICAO-compliant DTCs and avoid the interoperability issues associated with proprietary, standalone alternatives.

At SITA, this is a vital element of Digital Travel, informed by 25 years' experience issuing Electronic Travel Authorizations. Our vision is to bring together all stakeholders involved in the end-to-end travel journey to build an interoperable, standards-based identity ecosystem that is beneficial for the entire travel and tourism sector.

For more information, contact:
SITA Border Management

We would strongly recommend governments start making plans to issue ICAO-compliant DTCs and avoid the interoperability issues associated with proprietary, standalone alternatives.

[5] Ref. ICAO - https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Digital%20Travel%20Authorizations.%20%28New%29.pdf

SITA

Registered Office

SITA SC
2 Avenue des Olympiades
B-1140 Brussels
Belgium
Tel: +32 (0) 2 745 0517

Geographic Offices

Americas
600 Galleria Parkway
Suite 1000
Atlanta, GA 30339
USA
Tel: +1 770 850 4500

Asia Pacific
11 Loyang Way
Singapore 508723
Republic of Singapore
Tel: +65 6545 3711

Europe
Chemin de Blandonnet 10
1214 Vernier
Switzerland
Tel: +41 22 747 6000

Middle East & Africa
Holcom Building
Cornich Al Nahr
Beirut - Lebanon
Tel: +961 1 637300

WWW.SITA.AERO