IDEMIA

Shaping the future of digital travel credentials

Lessons learned from the world's first transatlantic DTC-1 pilot.

IDENTITY

POSTED ON 12.05.24

Few topics have been covered in recent identity industry events as often as Digital Travel Credentials (DTC). However, hardly any presentations and articles have come from the "inside" and been delivered by someone actually involved in a live pilot under operating conditions. Most of the information and advice still comes from suppliers that have no or very little experience outside the ivory tower of R&D.

Let us change this! Just recently, on behalf of IDEMIA Smart Identity, I had the honor of presenting the lessons learned from the first transatlantic DTC-1 pilot at the **ICAO TRIP symposium** in Montreal, Canada.

Here is what I presented:

Key fact 1: DTC offers tangible benefits to users and governments

This will come as no surprise to those in the industry who have worked on this topic for a while, but it is still worth mentioning the results from the pilot that IDEMIA Smart Identity was involved in have proven this to be true. A DTC, even if it is "just" DTC Type 1, ensures a safer and more convenient travel experience. Optimized border clearance processes and improved passenger flow lead to reduced costs for the border police.

Key fact 2: The lessons learned from the first transatlantic pilot are encouraging

IDEMIA Smart Identity was the technology provider of the first transatlantic DTC-1 pilot, carried out by a Dutch consortium and co-funded by the European Commission. While all actors anticipated this project to be far from smooth sailing, there were certainly obstacles to overcome that we will have a much stronger focus on in any upcoming projects. Overall, it became clear very quickly that we face an "iron triangle," aiming to achieve the best traveler experience, data security, and data privacy, equally, without compromise. This is surely the case in many identity use cases but, when international travel is concerned, this challenge takes on a whole new dimension.

Our key recommendations for future DTC projects:

1. **Putting the traveler at the center will drive adoption**
   No digital identity project will ever be successful if it is not set up with the end user at its center. A complex user experience, or just the smallest obstacles to get on board, will lead to the target audience abandoning

- the innovation and going back to the old, reliable ways—in our case, the physical passport.
  We need to think about the whole journey. Many different parties and systems are involved in international travel. All systems need to work with each other, give the same convenient and inclusive user experience, and work across different versions of technology (different generations of smartphones, operating systems, etc.). If just one element fails in this respect, the whole chain is weakened. This includes, as simple as it sounds, a huge focus on UX design, user guidelines, and tutorials for the end user.

2 – **Achieving highest security requires a focus on the underlying systems**
  The adoption of digital identities is driven by the user experience and the associated benefits (see point above), but only if the end user has trust in the process. Trust is created by the highest security in the systems involved. There is no doubt that biometrics play an essential role in the issuance and use of digital identities, but it goes beyond this. Multifactor authentication is only one example of protection measures to be built in across the whole process. The management of the ICAO Public Key Directory, the central repository for exchanging the information required to authenticate ePassports, remains particularly important, even in the case of a DTC.

3 – **Safeguarding data knows no compromise**
  A DTC solution will inevitably involve the storage and transfer of sensitive personal data, such as biometric information and travel documents. Compliance with data privacy regulation is essential—data privacy is non-negotiable. We must ensure that travelers have control over their personal data. This includes obtaining explicit consent for data collection, ensuring transparency in how the data will be used, and giving users the right to revoke consent or request deletion of their data.
  A reliable response to this challenge is, of course, data minimization. A DTC solution will collect and store only the minimum data necessary for identity verification and travel purposes and this for a limited duration of time. This aligns with data minimization principles in privacy regulations.
  Given that we talk about international travel, in our case between the Netherlands and Canada, data will be transferred across borders. Hence, compliance with regulations is necessary in all countries involved.

Why do I say that these lessons learned are encouraging?

Because these are not new topics in the identity ecosystem. Indeed, the complexity is extrapolated in the world of international travel in comparison to the creation of a national scheme, but the issues are not unsolvable. The key point remains that a digital identity is not “just” a digital version of a physical identity credential but is completely reliant on the performance and security of the underlying systems. Only a strong focus on, and experience with, the biometric systems needed will lead to successful implementation of a project.

Key fact 3: DTC is here to stay

With all this in mind, the feedback received from the pilot confirms: DTC is here to stay. The expected benefits have been confirmed and travelers are ready for the adoption of such an innovation. What is lagging behind is, as often, the regulatory framework, but even here the reality of such a pilot has increased political pressure and led to fruitful discussions.

More and larger pilots already planned will hopefully increase overall trust in this groundbreaking change in the way we travel. We, at IDEMIA Smart Identity, are certainly ready to apply our knowledge.

About the author: Sahy Rabarimeriarijaona is Product Manager for Mobile ID at IDEMIA Smart Identity.