Border control at most modern airports now mostly consists of simply placing the e-passport on a scanner

IDENTITY CONFIRMED

Nick Larter *reveals how digital passports are making travel experiences smoother*

From passports to ID cards to driver's licenses, many government documents already have a digital counterpart. But we are only using a small fraction of what digital identity technology can actually do. Its widespread use will not only open up countless new applications and benefits, but usher in a whole new level of convenience for travellers and authorities.

Since the introduction of the e-passport, there have been major technological advances and numerous successful e-government projects, such as the digital ID card or the introduction of RFID chips in driver's licenses. But despite these innovations, the reality is still far from digital. For example, most visits to government offices still involve making an appointment and showing up in person. And even though more and more citizens are using digital solutions to confirm their identity, the critical mass has not yet been reached, which could be an indication that the paradigm shift from physical to digital documents is complete. However, this is not just a matter of replacing physical documents with their digital counterparts. Rather, the greatest added value here comes from the coexistence of both and the freedom of the user to choose which option to use when and for what purpose.

With the advent of e-passports in the early Noughties, travel documents took a real leap forward in terms of security, ushering in a new era in the evolution of government documents. The new idea behind it: while the classic printed, physical passport with a photograph was susceptible to forgery and destruction, the same information about a person could be stored digitally, tamper-proof, and readable by authorised authorities. The digitisation of data that can be used to uniquely identify citizens also forms the basis for the large and important area of e-government – and thus for simplified and time-independent access to all types of government services. While digitisation is already making life much easier for federal, state, and local governments, the use of digital solutions to verify identities also holds great potential for making everyday life easier and more convenient – especially in the important area of mobility.

The world has never been travelled as much as this year, if the latest figures from the world of international travel are to be believed. In air travel alone, the number of passengers has risen steadily by almost five percent each year. Modern travel documents must meet a variety of daunting challenges. On the one hand, they must be secure and reliable, ready for their key role in curbing cross-border criminality. On the other, they must be convenient and efficient – ideally even automated – in order to effectively meet the modern traveller's expectations of a fast turnaround.

The e-passport is a good example of how the widespread use of digital identities can simplify many everyday processes. Gone are the days in Europe and much of the world when border officials checked each person individually, comparing photos and using stamps. Border control at most modern airports now mostly consists of simply placing the e-passport on a scanner – a process that speeds up the check, reduces the workload for staff and has become the new standard. The next logical step is now to transfer the information used on the passport chip, the digital profile, to a secure application on the smartphone. This will open up completely new use cases where people can verify and authenticate themselves online. In the future, they will be able to plan and carry out their entire journey digitally, from booking a taxi to checking in, to a train or automatically checking into a hotel using their smartphone as a room key – the seamless travel of tomorrow.

One day international air travel could also operate with far fewer points of contact than today. A major challenge here is to implement the necessary internationally recognised standards. Although many countries already use electronic passports as well as the corresponding back-end systems for automatic matching, not all countries are on the same level. However, since global interoperability is not only the purpose, but also a basic requirement for the passport, the same framework must apply worldwide. The solution comes from the International Civil Aviation Organisation (ICAO), which has issued a guideline for digital travel documents called Guiding Core Principles for the Development of Digital Travel Credential (DTC). The directive aims to ensure international compatibility of identity solutions, as well as the necessary security.

ICAO has also defined three crucial stages for the further development of the digital passport. In the first phase, which we are currently in, the information transferred from the passport to the smartphone is merely a supplement to the physical documents (DTC-Virtual Component), which remain the clear priority. In the second stage, the passport will have a digital formfactor counterpart (DTC-Physical component) that travellers can use as they wish – although carrying the physical document will still be mandatory. In the final phase, this will no longer be the case: travellers will be free to choose which option they prefer. However, a key aspect of timely implementation is social acceptance.

> THE EXISTENCE OF DIGITAL DOCUMENTS IS A PREREQUISITE FOR SEAMLESS TRAVEL

Digital versions of passports on smartphones are technically well developed, but in most cases, users are still not ready to use them as naturally in everyday life as traditional, physical passports.

Past changes and developments have shown that time plays an important role in the widespread adoption of new technologies. For example, contactless payment methods using smartphones are much more widely accepted today than they were a few years ago. People are more likely to accept new solutions if they trust the processes and the technology works smoothly. The same applies to the digitisation of personal documents such as bank cards, driver's licenses and passports, which requires new security standards.

If the device is stolen, criminals will have to jump through a series of hoops to gain access to the documents, from unlocking the device and logging into the application to biometric logins and multi-factor authentication. Owners can also remotely lock their smartphones or even wipe the contents. Anyone who takes someone else's wallet, on the other hand, has direct access to cards that their owners have to block manually and individually after losing them – often too late. No one wants to know that their ID card is in the hands of strangers or criminals, as identity theft has become a widespread problem in recent years. Digitising documents is a big step forward in terms of data security. However, only the government can issue legal proof of identity, the legal framework must be strictly adhered to, and the requirements for the underlying software must be correspondingly high.

For everyday use of digital government documents to become a reality, governments must focus on both regulatory compliance and security when developing solutions. Data security, protected transmission and

GONE ARE THE DAYS WHEN BORDER OFFICIALS CHECK EACH PERSON'S PASSPORT INDIVIDUALLY

secure communication with the back end are not just 'nice to have', but fundamental requirements. Then there is the interoperability factor with systems in other countries and their individual agencies. There can be no isolated solutions that work well within their own borders but are not team players. In terms of the software required, these tasks are challenging, but not uncharted territory. Service providers that specialise in working with governments are familiar with the high requirements and have the necessary expertise. In terms of technology, a lot can be done with the current state of the art – the situation is different when it comes to user behaviour. Experience shows that major societal changes, such as the shift to digital solutions in this case, take time.

The benefits of digital passports and other documents that can be used without their physical counterparts are obvious, not least from a security perspective. The number of use cases is not even foreseeable yet, as the number of applications increases with the number of users. For example, age verification at a self-checkout kiosk, which is already in use today, could relieve staff of manual checks and allow hotel guests to check in automatically, complete with no further interaction at the front desk. Another area that could benefit from digital documents in the future is healthcare – in conjunction with concepts such as digital patient records, many processes could be automated, saving time and effort for often overworked staff. The existence of digital documents is also a prerequisite for the idea of seamless travel, in which travellers go through the various processes of a flight, for example, without further contact with authorities or the provider. In this case, users could use their digital passports on their smartphones to register, apply for visas, pass through border controls and check in automatically. There is still a long way to go, but the many new solutions and use cases already demonstrate the enormous potential of digitisation and how it can simplify the processes of our everyday lives ●

Nick Larter is Senior Solutions Manager at Veridos.

Modern travel documents must meet a variety of daunting challenges

Picture credit: Veridos