

The Benefits of e-Passport Migration



CONTEXT

Following the events of September 11, 2001, the U.S. took the lead in accelerating the adoption of standards aimed at improving the reliability of traveler identification and the authentication of travel documents. As the most common travel document issued today, the passport is issued by one country and generally checked by another country. Therefore, more than any other identity document, the passport must follow standards of issuance and inspection in order to be the corner stone of an efficient and reliable system of traveler identification.

Those standards are set by ICAO (International Civil Aviation Organization), a UN specialized agency established in 1944. ICAO established and manages the administration and governance of the Convention on International Civil Aviation (Chicago Convention). Since 2011, ICAO has led several working groups and published the specification of the characteristics of Machine Readable Travel Documents in its ICAO Doc 9303. These rules are regularly reviewed, discussed and revised.

WHAT IS AN e-PASSPORT?

An e-Passport is essentially an enhanced version of the traditional passport.

The main difference to a classic Machine Readable Travel Document/Passport (MRTD/MRP) is the inclusion of a chip or integrated circuit (IC). The chip contains the holder's personal details like name, surname, date of birth, picture of the holder and nationality, plus the date of issuance and end of validity date. Additional biometric data like fingerprints or iris may also be included at the state's discretion.

Facial recognition is the only passport biometric used 100% of the time, but iris and fingerprint recognition are increasingly common. Electronic data, like a digital portrait picture, is considered more reliable than printed data, whatever the material or the printed definition. Therefore, the electronic passport is an inherently higher security document than the MRP.

Aside from the additional data it contains, the electronic passport relies on a range of security mechanisms, specifications or IT infrastructures to protect the data, provide access to it and manage the secure use of the passport itself.

The aims of these mechanisms, among others, are:

- Prevention of data skimming/eavesdropping on the communication between the chip and the reader
- Data authentication (to ensure the data was not altered)
- Chip authentication (to ensure that the chip is not manipulated or cloned)
- Data security (to ensure the information used by issuers / verifiers is properly shared through the use of Public-Key Infrastructure (PKI))



- Data skimming/ eavesdropping prevention

e-Passports are protected by Basic Access Control (BAC). BAC establishes an encrypted channel of communication between the reader and the chip — thus preventing eavesdropping — by using a password called an access key. This access key is generated via a combination of the basic information of the document holder and is presented in the Machine Readable Zone (MRZ) to make it easily readable by a device.

The basic idea behind the access key is that you need access to the holder page of the passport to be allowed to read the chip — like in a normal inspection environment where a traveler would hand over their passport to an agent.

Using BAC gives access to all information on the chip with one exception: fingerprints. Access to these is not possible without authorization from the issuing country. Keep in mind fingerprints are unique to each holder, eminently private and therefore very sensitive to handle.

- Document data authentication

The data authentication mechanism involves both a private key and a public key. The holder data is signed by the government with a private key and the immigration officer verifies that this data is actually from the issuing government by using that government's public key. The match of the two keys guarantees the data is as originally issued by the government.

In passport terms, this is called “passive authentication” and it checks the digital signatures and assesses the genuine origin and integrity of the content using the country certificate.

- Clone detection

While the previous step aims at proving the unaltered nature of the data itself, it does not guarantee the data, even when duly signed, was not copied and loaded from another passport.

The most common security mechanism for clone detection in passport is called “active authentication.” Simply put, it uses the chip's unique security number to guarantee that the chip interacting with the reader at the border is the same one that was used when the chip data were signed by the issuing country.

- Public Key Infrastructure

The secure and reliable exchange of certificates between the various countries issuing and verifying passports is based on:

- » The use of a specialized PKI applicable to travel document issuance and inspection, to guarantee the data signature and authenticity
- » The implementation of a Public Key Directory (PKD) to enable the distribution of certificates from all countries that are active members of the scheme



WHAT DOES AN e-PASSPORT ENABLE THAT AN MRP DOESN'T?

e-Passports are an enhancement to the many advantages derived from regular MRPs. What an MRP can do, an e-Passport can normally do better and much more securely.

So, let's review what it does better:

1. Secure and accurate identification of the passport holder

Fraudulently altering a passport's printed data is not enough to get it through inspection. Electronic data, which is protected by a digital signature, encryption, hardware and chip operating (software) security mechanisms provides a much higher level of trust to the traveling document.

The chip strengthens the holder profile verification as a whole by switching from a dual approach for the border control officer (comparing the information printed on the passport to the holder facing the officer) to a triple verification approach. The officer is equipped with a chip reader that allows him or her to compare: the holder versus the printed information, the holder versus the electronic data store in the chip and the printed information versus their electronic version stored in the chip.

2. Lower chances of forging the holder data stored in the passport

The personal information is duplicated and stored in two different forms: physical print and electronic encoding.

The data stored in the document are encrypted, and the chip and operating system are generally based upon technologies with proven resistance to basic and advanced hacking. The chip and its operating system are therefore used as a sort of data safe that is difficult to access.

Fraudsters would need to alter the document physically and electronically, and work on two different sections of the document: the personal data page material (paper or plastic) and the chip located in the booklet (generally in the back cover or in the plastic data page).

The various new protocols implemented in the chip and its operating system protect the chip data against reading, modifying and cloning, while the more classic printed sections of the document are still protected against physical or chemical alteration so that if they are modified it will leave a visible trace.

3. Protection against identity theft

The use of biometrics is a crucial move to fight identity theft. Biometrics are recognized as a primary tool for identification and they can be checked with readers rather easily. No more crossing borders with a stolen passport in which the photo has been replaced; now that the fingerprints or picture are stored electronically in the document, those data won't match during inspection when the fraudster fingerprints are compared in real time. No more impersonation of fraudster's rightful document owner with his stolen document.



4. Traveler-friendly and fast controls at the border

True for entry and exit, at the border or in an airport with the use of automated border control equipment like e-Gates. e-Gates can be totally contactless with facial recognition (cameras) or involve contact with fingerprint verification (FP readers).

These enables a faster and smoother flow of passengers compared to the manual inspection done at classic immigration check counters. It helps speed up the verification process and removes the human factor.

WHO BENEFITS FROM USING AN e-PASSPORT?

Various individuals and organizations benefit directly or indirectly from the introduction of electronic passports.

Travelers

Obviously, travelers have much to gain from going faster through security at the border. As e-Passports have become more common around the world — more than 135 countries out of 200 use them — they've allowed for increased convenience and a better user experience for the citizen traveling.

For business travelers, migrant workers and simple tourists, e-Passport programs facilitate traveling to places like the European Union (ETIAS program), or the U.S. (Visa Waiver Program) among others — enabling citizens or nationals from the participating countries to travel for tourism or business, for stays of 90 days or less, without obtaining a visa. As of today, an e-Passport is mandatory to enjoy the benefits of those schemes in the U.S. and recommended for the EU program.

Airlines, airports and port authorities

The ICAO main mission reads: "ICAO works with the Convention's 193 Member States and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector." With ICAO's emphasis on the aviation sector, it is no surprise that airlines, airports and port authorities benefit from the safe, secure and efficient transportation of travelers.

e-Passports facilitate the speed of the flow of passengers, and indirectly help to cut down the bottleneck that is border crossing and the administrative tasks like arrival form completion. Who has not experienced spending as much time waiting for their turn to cross a border at immigration as they actually spent traveling?

While an e-Passport doesn't necessarily cut the paperwork or expand the border crossing section in an airport, it opens the door to automated border crossing technology that reads electronic passports from any country. It also facilitates the quick processing of passengers to free room in airports, reduce the logistical impact of traveling and make current airport structures able to handle more traffic with the same resources.

State and government agencies

Since e-Passport programs are decided by governments, usually via their ministry of foreign affairs, and managed by dedicated agencies on behalf of the government, their benefits of using e-Passports are primarily security considerations and state-to-state agreements on visas.

Business, migrant and tourist travel ease impact a state economy in many ways — through the tourism industry or bilateral trade ease the impact on a state economy between two countries for example.

Ultimately, the standardization of biometrics and other verification facilitates cooperation between states via interoperable, compatible citizen data.

Let's list a few concrete benefits:

Advanced detection — Border crossing control benefits strongly from the capability to detect fraudulent or false passports. The use of readers and the consistency of the electronic data increases the quality of the inspection and allows detection of the improper use of documents, thus aiding the fight against crime and illegal immigration.

Databases — the use of modern biometrics in the issuance system and in the issued document itself is a first move in the creation of consistent and standardized citizen profiles in a given country. Those standards are international — the ICAO standard for travel documents is used very widely in most identity document schemes, like national ID cards for picture standards — and used across all countries working with ICAO. Governments can build databases with formatted data that can be efficiently exchanged or cross checked in cooperation with other countries. The data of partner countries can also be used to monitor high-risk categories of travelers, as well as share alerts on documents and profiles of travelers.

Quality of the issued document — the electronic passport document goes hand-in-hand with an adapted, upgraded system that checks every step of the document issuance. With the increased amount of information used in an electronic document comes the need for an IT system to manage the whole process of application, creation and issuance. It involves, for example, the management of signed certificates, but also capturing, processing and vetting the data during the document's early creation stages. Such a system evaluates the consistency of the data printed and loaded electronically in the chip, consistency of the personal data captured during application, and the data delivered in the issued document. Finally, the system can confirm the data of the holder when receiving his document via simple fingerprint or face check, electronic signature for the data, etc. The delivered document is an exceptional piece of work that has gone through a stringent process of checks and double checks to guarantee it's going to interact properly in various verification conditions.

Cost efficiency — The automation of the check decreases the time spent per inspection and improves the level of security. Agents cannot manually verify the matching of hash or signature in an electronic passport. The electronic check also decreases the need to use law enforcement agents for basic checks, reducing hiring needs and training for agents, freeing resources and time for other more complex tasks and simply reducing the overall cost of inspection and allocated infrastructure.

TAKE AWAYS

While migrating to an e-Passport could present a few challenges in terms of expertise, it is worth noting that it has been done in more than 2/3 of the countries in the world since its first implementation in 2008. There are recognized experts in the market with the hands-on experience and successful track record to assist countries choosing to take advantage of the many benefits of e-Passports.

Make no mistake, the benefits are very significant. An e-Passport significantly improves the security of the citizen's travel documents, facilitates the circulation of passengers in various part of the world, lowers hurdles to trade and business mobility, enhances the tools at hand for travel monitoring and gives a set of well-accepted standards for cooperation between countries.

Most importantly, the migration to an e-Passport is also the first step in a wider digital transformation of a country via the implementation of the systems required for other digital documents like n-ID cards, driving licenses, civil registry and many more.

Visit us at hidglobal.com



hidglobal.com

© 2020 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2020-04-29-cid-hid-benefits-e-passport-migration-wp-en
PLT-05145