A Look Into the Benefits and Security Measures of ePassports

INTRODUCTION

Passports have been a primary method for identifying travelers crossing borders for centuries. Although there have been many advancements in passports over time, a major leap forward was taken with the introduction of ePassports. This paper breaks down how ePassports benefit governments, travelers and travel authorities — and explains some of the technical details behind their stringent security.

WHITE PAPER

WHAT IS AN ePASSPORT?

An ePassport is essentially an enhanced version of the traditional passport.

The main difference between an ePassport and a classic Machine Readable Travel Document/ Passport (MRTD/MRP) is the inclusion of an electronic chip or integrated circuit (IC) in the ePassport. The chip contains the holder's personal details like name, surname, date of birth, picture and nationality, plus the date of issuance and end of validity date.

BENEFITS OVER TRADITIONAL PASSPORTS (MRPS)

ePassports are an enhancement to the many advantages derived from regular MRPs. What an MRP can do, an ePassport can normally do better and much more securely.

Here are the benefits for using an ePassport:

1. Provides secure and accurate identification of the passport holder

Electronic data, which is protected by a digital signature, encryption, hardware and chip operating (software) security mechanisms provides a much higher level of trust. 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 uses a chip reader to compare the holder, the printed information, and the electronic data stored on the chip for consistency.

2. Lower chances of forgery

The personal information is duplicated and stored in two different forms: physical print and electronic encoding. Fraudsters would need to alter the document physically and electronically. They would have to change 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 data stored in the document are encrypted, and the chip and operating system use technologies that resist basic and advanced hacking. They keep the data safe and difficult to access.

The various new protocols implemented in the chip and its operating system protect the chip data against unauthorized 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

Biometrics are crucial for fighting identity theft. They are 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's fingerprints are compared in real time. No more impersonation of the rightful document owner with his stolen document.

4. Traveler-friendly and faster border control

eGates enable 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. eGates can be totally contactless with facial recognition (cameras) or involve contact with fingerprint verification (FP readers).

OVERVIEW OF ePASSPORT SECURITY MECHANISMS

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
- 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)

ePassports 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 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.

Additional security mechanisms (beyond BAC) protecting ePassports, include:

- 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 (PKI)

  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 International Civil Aviation Organization (ICAO).

BETTER FOR TRAVELERS, GOVERNMENTS AND TRAVEL AUTHORITIES

TRAVELERS

Obviously, travelers have much to gain from going faster through security at the border. As ePassports 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 traveling experience.

For business travelers, migrant workers and simple tourists, ePassport programs facilitate traveling to places like the European Union (ETIAS program), or the U.S. (Visa Waiver Program). They help 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 ePassport is mandatory to enjoy the benefits of those schemes in the U.S. and recommended for the EU program.

AIRLINES, AIRPORTS AND PORT AUTHORITIES

ePassports improve passenger flow, and indirectly help to cut down the wait time for border crossing and the administrative tasks like arrival form completion.

While an ePassport 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

Business, migrant and tourist travel ease impact a state economy in many ways — through the tourism industry or bilateral trade between two countries, for example. Ultimately, the standardization of biometrics and other verification facilitates cooperation between states via interoperable, compatible citizen data.

AGENCIES

"The appeal of ePassports, to the government agencies that manage them, is primarily related to border security and state-to-state agreements on visas."

EMBEDDED WITH SECURITY TO EASE THE WAY TOWARDS WIDER DIGITAL TRANSFORMATION

More than 2/3 of the countries in the world have adopted ePassports since their first implementation in 2008. An ePassport significantly improves the security of the citizen's travel documents, helps with passenger flow, lowers hurdles to trade and business mobility, enhances the tools for travel monitoring and gives a set of well-accepted standards for cooperation between countries.

The migration to an ePassport is 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.

LEARN MORE

To learn more about migrating to ePassports visit ***hidglobal.com/products/epassports-and-eid-cards/epassports***.

HID
hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108

part of ASSA ABLOY