ePassport Frequently Asked Questions

A Smart Card Alliance Identity Council Publication

Publication Date: March 2009
Publication Number: IC-09001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

FAQ Table of Contents

ePassport Frequently Asked Questions

This frequently asked questions (FAQ) document was developed to answer questions about how the ePassport works and what technology is used to protect an ePassport holder's personal information.

The answers are focused on the United States ePassport implementation. Other countries may have implemented other options with their ePassport initiatives and would answer these questions differently.

In addition, the questions and answers apply only to the ePassport and **not** to the Passport Card (a different identity document also being issued by the Department of State).

1. What is an ePassport?

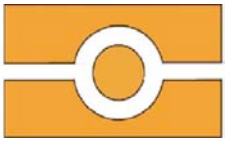
The electronic passport, or ePassport, is the same as a traditional passport book with the addition of a small, embedded integrated circuit (or chip). In the United States and many other countries, the chip is embedded in the back cover. The chip stores:

- The same data visually displayed on the data page of the passport;
- The passport holder picture stored in digital form;
- The unique chip identification number;
- A digital signature to detect data alteration and verify signing authority;
- Additional data, as defined by specific issuing governments.

Standards for the ePassport have been established by the International Civil Aviation Organization (ICAO)[1] and are followed by all countries implementing ePassports.

2. How do I know if I have an ePassport?

All ePassports can be recognized by the internationally recognized symbol that is printed on the front cover.[2] This electronic passport symbol identifies the passport as an ePassport. The symbol is also displayed at border crossing stations that have the capability to process ePassports.



3. Is an ePassport the same as a Passport Card?

No. The ePassport is a replacement for the traditional passport book that can be used for travel and border crossings globally. ePassports follow standards established by the International Civil Aviation Organization and are being issued by many countries around the world. The ePassport uses secure RF-enabled contactless smart card technology to protect citizen personal information and provide strong overall security for the passport document. U.S. State Department information about the ePassport can be found at http://travel.state.gov/passport/eppt/eppt_2498.html.

The Passport Card resulted from the U.S. Western Hemisphere Travel Initiative. It is issued only to U.S. citizens and can be used only to enter the United States from Canada, Mexico, the Caribbean, and Bermuda at land border crossings or sea ports-of-entry. The Passport Card uses a completely different RF technology – an RFID tag that allows unique Passport Card information to be read from long distances. Information about the Passport Card can be found on the U.S. State Department web site at http://travel.state.gov/passport/ppt_card/ppt_card_3926.html.

This FAQ applies only to the electronic passport and not to the Passport Card.

---

[1] Additional information can be found at http://www2.icao.int/en/mrtd/Pages/default.aspx.

[2] The symbol is defined in the ICAO Doc 9303 Machine Readable Travel Document specification.

4. How do I get an ePassport?

When you apply for a passport or renew any passport in the U.S. today, you will be issued an ePassport. The ePassport is quite different visually since it contains redesigned booklet pages and has the international ePassport symbol. Please refer to the State Department's web site for more details.[3] As before, you will receive a new passport number each time you renew. The book number will now match the passport number and both of these will be the same as the number programmed into the ePassport chip.

5. Are ePassports from all countries the same?

No. All ePassports follow the common ICAO standard. However, countries implement ePassport programs according to their specific policies and may implement different options specified in the standard. This results in differences among country implementations of ePassports even though they all conform to the ICAO specification.

6. Are U.S. ePassports more secure than traditional passports?

Yes. The ePassport provides the border protection officer with a new tool to help determine the presenter's identity by adding the electronic version of the printed document.

With the new booklet design that the State Department introduced with the ePassport, new printing features, and secure microcontroller chips incorporated into the booklet, the difficulty of passport forgery has significantly increased.

ePassports now include digital **and** physical security technologies that are integrated together to provide significantly higher levels of security. ePassports use advanced technologies that secure identities and new processes throughout the entire chain of trust – from manufacturing to use of the ePassport.

7. What security measures are built into an ePassport?

Security measures are found throughout the ePassport system, from the production of the book itself to the policies and procedures in place at border crossings.

Starting with the document, the U.S. ePassport is manufactured by the government, in government-owned facilities. No one outside the government knows the full "recipe" which includes special papers, inks, and manufacturing techniques. The embedded chip is a secure microcontroller with advanced cryptography and built-in sensors to detect attacks.

When the ePassport is personalized and issued, the data which has been written to the chip is signed by the issuing authority using their country signing key. (This is the digital equivalent to a public notary's seal certifying a document.) Once manufactured and personalized, no information can be changed.

The ePassport is designed to be read only when open and after a successful read of the machine-readable zone (MRZ) by an ePassport-enabled reader.

Last but not least, governments, manufacturers, national printers and control personnel have enhanced their passport manufacturing, delivery and control processes to set up a stronger chain of trust. These improved processes protect citizens from identity theft and prevent terrorists from obtaining official-looking passports with false identities.

Anyone wanting to make an ePassport copy would need to have the chip, the data, and all of the manufacturing components and know-how. But without the government private cryptographic key

[3] http://travel.state.gov/passport/passport_1738_2.html

required to digitally sign all of the information, anyone trying to use a forged passport would be stopped when the cryptography verification would fail.

8. *How is an ePassport used at border control?*

Figure 1 shows how an ePassport is used at border control.

9. *What if I lose my ePassport?*

As with traditional IDs or passports, it is of utmost importance to protect your own identity documents. Identity documents should never be left unattended or passed to someone else…whether they are electronic or traditional!

Currently, if someone loses a traditional passport, the loss must be reported to the appropriate authorities. The same applies if you lose an ePassport. At border control, it is easier to track whether any lost or stolen ePassports are being used.

10. *Is reading an electronic passport considered an attack and/or hack?*

Reading the information contained in an ePassport is neither an attack nor a flaw in security. Reading and copying the electronic data in an ePassport are not threats and are essentially the same as reading and photocopying a traditional paper-only passport that has been opened.

The new ePassports are designed with multiple layers of security. The fact that the printed information is an exact match to the digitally-protected electronic information makes the new ePassport much more secure and resistant to fraud.

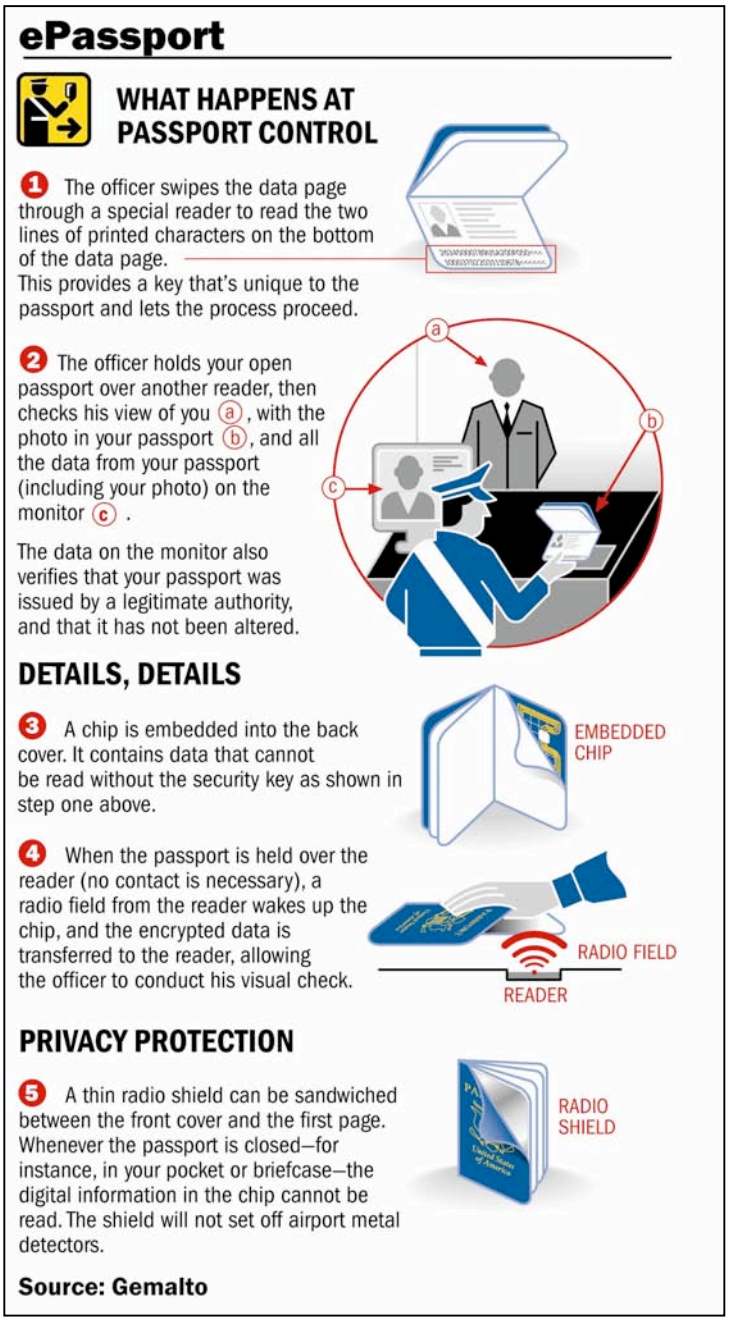


Figure 1: ePassport Use at Border Control

11. *Can anyone "perfectly clone" an ePassport as written in the press?*

ePassports are designed with multiple security features.

First, an ePassport is made of special paper incorporating high security printing features. In much the same way that money is printed and produced, these sophisticated features are incorporated on special paper and supplies are protected by sophisticated means.

In addition to these physical printing security features, ePassports also have a small, embedded integrated circuit. When an ePassport is created, the same information is both securely printed on the paper and securely written to the chip. The information on the chip is digitally signed by the issuing country's passport authority. (This is the digital equivalent to a public notary's seal certifying a document.)

To successfully clone an ePassport, a criminal would need to obtain both the security paper and an appropriate chip. The criminal would then need to create a complete ePassport book, embed the chip and write the digitally-signed data into the chip – and to do this in such a way that the resulting ePassport would look authentic to a border crossing agent. While this is technically possible, it would be extremely difficult to make an exact duplicate of an existing ePassport.

it is also important to remember that cloning an ePassport would be equivalent to someone using a copy of your ePassport without your knowledge. In order for your ePassport to be used by someone else to assume your identity, the other person would have to look just like you. For this reason, cloned ePassports do not present a high level of risk.

12. Can anyone change the data in an ePassport?

In the past, it was possible to replace the photograph glued in the passport book and/or alter the data printed under the laminate. With an electronic passport, advanced techniques are used to print the data page, and the data and photograph are also written electronically to the chip. So, for someone wanting to change the data, the first hurdle would be to successfully alter the information in both places, and to do so without attracting attention as a result of obvious tampering.

But, even if someone were able to introduce alternative or fraudulent data on a substitute chip (as some hackers have claimed), the fake ePassport would not pass border control. Any change to the data invalidates the ePassport since the digital signature would no longer match the stored information. So the second, and bigger, hurdle would be creating the correct digital signature to match the new data. Most passport authorities lock the data stored in the ePassport once it has been programmed so that the data cannot be altered. They then digitally sign the data with their country signing key, which is very well protected.

13. Is there a risk today of a copy of your ePassport being used by an impostor at border control?

No. The ePassport shows your picture, your name and other information proving who you are; this information is of no use unless the attacker is your identical twin or tries (and succeeds) to alter some of the information and use the resulting ePassport for someone else. An ePassport copy is not useful to a criminal or impostor. The passport information on the chip can't be changed without being detected. An ePassport copy would be of no use to anyone else, because your picture is on the chip and it is printed in the ePassport and the impostor is not you. This situation is no different from an impostor trying to use a lost or stolen paper passport without alteration. The entire ePassport program is designed to eliminate the risk of someone altering or using someone else's passport credential, and the security mechanisms put in place work well.

WHY IT IS NOT A RISK

The objectives of the global ePassport program were to make passports virtually impossible to counterfeit and to prevent anyone other than the passport owner from using the ePassport. The ePassport program achieves these objectives in two ways.

First, the information on the printed page, including the bearer's photograph, is stored on the chip and then displayed on a screen at passport control. By comparing the digital information, the printed passport and the person, passport control staff can confirm that everything is OK. They will immediately see a discrepancy if someone is attempting to use someone else's ePassport chip information.

Second, the information on the chip is digitally signed by the issuing country's passport authority. This means that if the information changes in any way after the ePassport is issued, the alteration would be detected at passport control. It also means that any attempt to create a fake ePassport credential will be detected.

14. What if a criminal copies the data onto another chip or device and inserts it in a different passport book?

If someone were to use a copy of the data on another chip or device with a different data page or photo, the border inspection equipment would highlight this discrepancy and alert the inspector. This electronic verification comes in addition to traditional visual checks, which are still carried out by the inspector.

A chip or device with a copy of ePassport data will not work with a different ePassport book. In addition to the previous security measures described, additional security features prevent this risk.

ePassport data is protected with a technique called Basic Access Control (BAC). At border control, the ePassport must be opened and the block letters printed at the bottom of the data page (called the Machine Readable Zone, or MRZ), must be read first.

The contents of the MRZ contain a key which is used to access the chip; the chip is only allowed to communicate with a reader if the key matches.

The MRZ data is not secret information. It is simply a representation of some of the printed information on the data page. The MRZ data allows computers to electronically read the printed information accurately.

If the MRZ information printed on the data page does not match the key the chip is expecting, communication with the ePassport chip cannot take place and no digital information is provided.

15. Can anyone read my ePassport without me knowing it?

When you physically give your ePassport to someone else (for example, to border control or to a hotel), they are able to open the ePassport book and visually read all of your passport information. If they had an ePassport-enabled reader, they would also be able to read the data from the electronic chip.

If they did not have physical possession of your ePassport or if your ePassport book is closed, then the answer is no. U.S. ePassports have a metallic RF shield built into the covers to prevent anyone from reading the ePassport's electronic chip. This shield completely protects the chip from being read or detected while the ePassport book is closed and prevents anyone from reading the information in your ePassport without your knowledge.

The ePassport book is designed to be handed to someone and opened before any information stored on the chip is read. Then, the MRZ must be electronically read and presented to the ePassport chip before the chip will communicate the passport information. All information exchanged between the reader and the ePassport chip is also encrypted using Basic Access Control, providing yet another layer of protection.

16. What if someone tries to read my ePassport without my consent?

The ePassport incorporates multiple security elements to prevent reading of private data without the citizen's consent. First, an electronic reader must be brought within three inches of an ePassport in order to function. Secondly, even if a reader attempts to read data at that close distance, the ePassport would only return a randomly generated unique identifier (which changes with each attempted read) with a request for the ePassport-unique MRZ data that is printed on the inside of the ePassport. The MRZ contains information that must be used by an external device to form the correct access code to wake the passport up. Thirdly, the U.S. ePassport

incorporates a metallic shield that prevents access to the data when the booklet is closed. These security elements help ensure that the ePassport will be read only when physically presented, the booklet opened, and the MRZ scanned by a properly configured reader.

17. Can someone track my ePassport when it's in my possession?

The ePassport employs an untrackable, randomly-generated, unique identifier that changes each time the ePassport is read. Any data unique to a particular ePassport can only be read after first obtaining the ePassport MRZ data that is printed on the booklet data page and only accessible when the ePassport is physically presented to a reader (for example, at a border crossing point). Additionally, the U.S. ePassport incorporates a metallic RF shield that prevents reading the ePassport when the booklet is closed. These security features serve to effectively block any tracking.

18. How can I tell if the metallic shield in my ePassport is actually working?

The U.S. ePassports contain a metallic RF shield within their covers. If the book is closed, the shield will inhibit any detection of the chip. Since the shielding material is a passive material and is an integral part of the book construction, it should remain functional for the expected life of the ePassport.

19. Is fingerprint information stored in the ePassport? How would fingerprint information be protected?

The U.S. ePassport does not contain fingerprint information today. According to the Department of State, the U.S. has no current plans to add fingerprint information to the ePassport.

Advanced Questions

20. What is Basic Access Control and how does it work?

Basic Access Control (BAC) is an optional security mechanism defined in the ICAO ePassport specification to ensure data integrity and to ensure that only authorized parties can read personal information from ePassports. BAC also includes the ability to perform an active authentication check to detect cloning.

BAC uses data such as the passport number, date of birth and expiration date to negotiate a session key. This key can then be used to encrypt communication between the ePassport's chip and a reading device. This mechanism is intended to ensure that the owner of an ePassport can decide who can read the electronic contents of the ePassport. The mechanism was first introduced into the German ePassport on 1 November 2005 and is now also used in many other countries (including the United States ePassport since August 2007[4]).

The key used to encrypt the BAC communication is extracted by optically reading the bottom of the ePassport printed page called the machine readable zone, or MRZ. Because physical access to the ePassport is needed to read the MRZ, it is assumed that the ePassport's owner has given permission to read the ePassport. Equipment for optically scanning the ePassport MRZ is already widely used. It uses an optical character recognition (OCR) system to read the text which is printed in a standardized format.

21. What is Extended Access Control (EAC), and how does it work?

Augmenting BAC, Extended Access Control (EAC) is an additional security access mechanism defined in the ICAO ePassport specification to meet data protection requirements and to help

[4] http://travel.state.gov/passport/eppt/eppt_2788.html#Eleven

protect the privacy of additional biometric data (for example, fingerprints). Implementation is planned in future generations of ePassports and will be country-specific. EAC also ensures that access to biometric data is only possible if allowed by the issuing country.

EAC uses additional cryptographic mechanisms to protect biometric data from being retrieved without proper authorization. An ePassport equipped with EAC protects the additional biometric data using encryption. Each ePassport will have unique keys to protect access to the sensitive information.

With the help of EAC, ePassport readers at ports of entry can be authorized to read data, and selective access rights can be defined. The retrieval of fingerprints requires sovereign powers (e.g., the permission of the country which issued the ePassport). EAC makes it possible to define whether an authorized entity is able to access the additional biometric information, with the issuing country deciding whether another country can access the data.

According to the Department of State, the United States has no plans to incorporate EAC or citizens' biometric data into ePassports at this time.

22. How do countries determine that an ePassport is valid? What is a Public Key Directory?

Countries determine that an ePassport is valid through a number of different techniques.

First, the ePassport must be current (not expired). Each ePassport has an expiration date printed on the document and also written onto the electronic chip. The expiration date on the chip is protected against modification or forgery by a digital signature. The digitally-signed expiration date can be verified by electronic passport readers.

Second, the information is checked to determine if it is authentic. The ePassport printed material security features (e.g., watermarks, security threads, papers and inks) are checked to determine authenticity. ePassport data (of which the expiration date is one element) is also protected by a digital signature.

Third, the country must determine if the issuer (i.e., the "printer" of the information on paper and on the electronic chip) is trusted. This is accomplished by checking the issuer's digital signature. Countries use the ePassport system's public key infrastructure (PKI) to do this check. This requires that the country checking the passport obtain a copy of the issuer's signing certificate ahead of time so its key can be compared with the key that signed the information in the ePassport. This would need to be done for each issuer (i.e., each country whose ePassports are accepted); the information (i.e., each country's signing certificate) must also be kept up to date to ensure that it is still valid.

Managing individual relationships to obtain this information from all other countries is a complex task. ICAO has established a Public Key Directory, or PKD, as part of the global system for ePassport validation. Every country issuing ePassports digitally signs the data with the corresponding country signing keys. The ability to verify a country's digital signature is an essential element of ePassport validation, and the PKD provides a means for border control authorities to verify that the digital signature on an ePassport is indeed valid.

The ICAO PKD has been established to support the global interoperability of ePassport validation and to act as a central broker to manage the exchange of certificates and certificate revocation lists among countries. This central role helps to manage the otherwise onerous public key certificate exchange activity that would take place among the many countries issuing ePassports.

Additional information regarding the ICAO PKD, including participating countries, can be found at: http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx

Publication Acknowledgements

This document was developed by the Smart Card Alliance Identity Council to answer questions about how the ePassport works and what technology is used to protect an ePassport holder's personal information. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank Identity Council members for their contributions to this FAQ, including: Computer Sciences Corp. (CSC); Gemalto; Giesecke & Devrient; HID Global; IBM; ID Technology Partners, Inc.; IDmachines; Infineon Technologies; IQdevices; Jellen Ventures Inc. (JVI); NXP Semiconductors; Oberthur Technologies; Probaris; SAIC; Sun Microsystems; TrustBearer Labs; Unisys

Special thanks go to the following Identity Council members who participated in the development of the FAQ:

- **Linda Brown**, Infineon Technologies
- **Kathleen Carroll**, HID Global
- **Myeong Choi**, Giesecke & Devrient
- **Edward Clay**, Sun Microsystems
- **David Corcoran**, TrustBearer Labs
- **Sal D'Agostino**, IDmachines
- **Walter Hamilton**, ID Technology Partners
- **Patrick Hearn**, Oberthur Technologies
- **Larry Jellen**, JVI
- **Bryan Ichikawa**, Unisys
- **Richard Lazarick**, CSC
- **LaChelle Levan**, Probaris
- **Gilles Lisimaque**, ID Technology Partners
- **John McKeon**, IBM
- **Cathy Medich**, Smart Card Alliance
- **Neville Pattinson**, Gemalto
- **Steve Rogers**, IQdevices
- **James Sheire**, NXP Semiconductors
- **Chris Williams**, SAIC

The Smart Card Alliance would also like to thank Gemalto for the Figure 1 graphic.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.