Security of Romanian Electronic Passports: The Protection of Personal Data in the Digital Age

Aurelian-Gabriel BĂDIȚĂ

Border Police Department, "Al. I. Cuza" Police Academy, Bucharest, Romania

aurelian.badita@academiadepolitie.ro

Abstract

Highlighting the evolution and importance of electronic passports in Romania, respectively the security risk associated with cyber attacks against the system for issuing these documents, represents a first pillar in the development of strategies to protect national security. Adopting a proactive approach in managing cyber risks in ensuring the security of the electronic passport issuance system, respectively the security of citizens' personal data, is necessary to provide an optimal climate of trust, both for the national/European/international order and security structures, and for the well-being of the citizens who request such documents. It can be seen that attackers or impostors develop various strategies to identify and gain access to data in electronic passports in order to exploit or compromise them. Many of them resort to different methods of accessing the personal data of electronic passport holders in order to falsify them and use them to cross the state border, respectively to alienate them to other potential criminals who want to evade border control. The structures responsible for issuing e-passports implement state-of-the-art high-performance electronic security equipment and systems to counter cyber-attacks, but permanent security methods are required, as attackers resort to modern advanced methods of unauthorized access.

Index terms: evolution of passports, electronic passports, cyberattacks, protection of personal data, consequences of cyberattacks

1. Introduction

The evolution of travel documents, from a simple document, which certifies the right of a person to cross the state border, to an electronic document, which contains biometric elements with an integrated chip, where information on the holder's data is stored, has experienced a real rise in the digital age.

The term passport was not yet assigned to travel documents since it was attested as a travel document. Thus, in the period of Antiquity and the Middle Ages, the documents that served the holder to cross the state border were called differently[1].

The term passport first appeared in England in the 15th century, but the etymology of the word comes from the French *passer* (to pass) and *port* (to carry), as French was a language of international diplomacy at the time.

---

[1] Online source: https://pasapoarte.mai.gov.ro/wp-content/uploads/2021/03/comunicat-ZiuaPAS-2011.pdf, accessed on August 4, 2024 - "*salvconducte, scrisori adeveritoare, cărți de pribegie, răvaşe, sineturi, teşcherele, foi de circulație, foi de călătorie, pasuri, pasuşuri sau paşapoarte*"

"*The United Kingdom and France are two countries which both claim the right to have invented the passport, in the contemporary sense of the term*"[2].

In United Kingdom, reference has been made since 1414 to the travel document, but entitled *laissez-passer* (*free passage*), and in France the travel document has been called a *passport* since 1420[3].

As human migration has taken place throughout history for a variety of reasons, driven by a variety of factors such as climate change, trade, exploration, conflict, etc., state authorities have tightened the conditions of travel.

Also, in order to have a control over persons migrating to/from the territory of a state, the authorities of that state have developed policies and strategies on the security of fraudulent documents by adopting legislation on the circulation of these documents.

Therefore, there are now a number of international, European and national rules in place to make it more difficult to fraud these travel documents, and travel documents with biometric data and high performance security features are being put into circulation.

2. Evolution from traditional to electronic passports

A reference moment regarding the evolution, both from a technical and legislative point of view, of passports, is the period following the events of December 1989. Thus, after this period, the passport experienced a real transformation as the national borders were opened to Romanian citizens.

However, in order to be recognized outside Romania, passports had to be made according to international standards.

A first model of passport complying with international standards was issued "*from June 1994*", which contained a computerized - double laminated - tab.

This passport is known as the *1993 model* since it was put into circulation following the adoption of Government Decision No. 757/1993[4].

The next passport model, *model 2001*, was put into circulation based on Government Decision no. 460/2001[5], on 21 January 2002. To which significant changes have been made, including the digital printing of the holder's photo on the computerized file[6].

A landmark moment in terms of the development of a legislative framework and the introduction of passports containing biometric data was the unfortunate moment of the terrorist attacks in the USA, on September 11, 2001. Thus, for the first time, the United States launched on May 14, 2002 through the Visa-Waiver program the document "*Enhanced Border Security and Visa Entry Reform Act of 2002. Aliens*"[7], and in order to allow third citizens to enter the US territory, they were required to have passports with biometric data and containing ICAO[8] standards.

---

[2] Cornea, V., "*Evoluția și implicațiile sociale ale pașaportului: de la scrisori de liberă circulație la pașapoarte de aur*", published in The Scientific of Cahul State University B.P. Hașdeu: Social Sciences, no. 1(11), p. 52, 2020, online source: https://www.researchgate.net/publication/341357883_Evolutia_si_implicatiile_sociale_ale_pasaportului_de_la_scrisori _de_libera_trecere_la_pasapoarte_de_aur_The_evolution_and_social_implications_of_the_passport_from_the_free_pas sage_letters_to_golden_pa, accessed on August 5, 2024

[3] Cornea, V., op. cit., p. 50

[4] Government Decision no. 757 of December 30, 1993 on the introduction into circulation of the new Romanian passports, published in the Official Gazette no. 24 of January 26, 1994

[5] Government Decision no. 46 of May 9, 2001 on the introduction into circulation of new types of Romanian passports, published in the Official Gazette no. 272 of May 25, 2001

[6] Costea, S.G., Porojan, M., Sbîrlea, C. & Popa, V., "*Regimul juridic al liberei circulații a cetățenilor români*", printed by C.N. "Imprimeria națională" S.A., Bucharest 2019, p. 73

[7] Online source: https://www.govinfo.gov/content/pkg/PLAW-107publ173/pdf/PLAW-107publ173.pdf, accessed on August 6, 2024

[8] ICAO – The International Civil Aviation Organization

These standards were set out in the document entitled "Document 9303"[9] –*Technical specifications for reliable travel documents* and defining precise requirements for electronic passports, including specifications on the integrated chip, formats and types of data stored, data encryption, security features, as well as global interoperability requirements.

Thus, Regulation (EC) No 2252/2004[10] was also adopted at EU in order to start the procedure for putting electronic passports into circulation and meet ICAO standards.

Starting with December 31, 2008, the electronic passport containing a non-contact chip with biometric data was put into circulation.

This 2008 passport model is also called *the first generation of electronic passports* and has biometric data implemented on the memory medium (E.g.: facial photography and dactyloscopic impressions), biographical (e.g. date and place of birth) and unique information of the holder (example: personal identification number), but also the unique passport data (example: document number).

The longest-standing Romanian legal act on the basis of which this passport model was issued and which is still in force today is Law 248/2005[11].

Due to the changes that occurred in the context of adapting to the current needs of modern society and the requirements imposed by the legislation in force, the normative act has undergone several additions and amendments, but without major changes on the substantive aspects.

Another passport model, also called *the second generation of electronic passports*, was put into circulation in May 2010, with the same format, but with higher security features than the previous one.

Starting with January 1, 2019, *the third generation of electronic passports* was put into circulation because it was necessary to issue a new passport model, both in terms of renewal and insertion of new security elements, and due to the fact that 2018 marked the 100th anniversary of the Great Union[12]. At the same time, the provisions of Law no.146/2016[13] required the public authorities to replace the coats of arms and seals existing at that time.

This model passport is the last type of document to be issued at national level and which includes advanced security features.

3. What electronic passports are?

A definition of electronic passports can be deduced from the wording of Article 6, paragraph (4) of Law 248/2005, which states that they are travel documents that "are the property of the Romanian state and provide proof of identity, citizenship, status, and the holder's right to travel abroad"[14].

Electronic passports are travel documents that contain an electronic chip that stores biometric and personal information of the holder, as well as document data.

This information may include dactyloscopic impressions, also called fingerprints, the holder's facial photograph, as well as other data visible on the computerized file.

---

[9] Online source: https://www.icao.int/publications/Documents, accessed on August 6, 2024
[10] Council Regulation (EC) No 2252/2004 of December 13, 2004, on security standards and biometrics in passports and travel documents issued by Member States, published in the Official Journal of the European Union No L 385/1 of December 29, 2004, as amended and supplemented
[11] Law no. 248 of July 20, 2005 on the regime of free movement of Romanian citizens abroad, published in the Official Gazette no. 682 of July 29, 2005, with subsequent amendments and additions
[12] Online source: http://centenar.gov.ro/web/marea-unire/, accessed on August 6, 2024
[13] Law No 146 of July 12, 2016 amending Law No 102/1992 on the national coat of arms and state seal, published in the Official Gazette No 542 of July 19, 2016
[14] Law no. 248 of July 20, 2005 on the regime of free movement of Romanian citizens abroad, published in the Official Gazette no. 682 of July 29, 2005, with subsequent amendments and additions

All of this information and data is included on the chip to improve the security and reliability of passports and also to quickly identify the identity of the document and the user.

Electronic passports are designed to prevent fraud and facilitate the border control process.

The implementation of ICAO standards ensures that electronic passports comply with a common set of technical and security requirements, while facilitating their mutual recognition internationally. These requirements also enhance the security of the holder's information and identity.

At national level, electronic passports are produced by *"Compania Naţională - Imprimeria Naţională - S.A., in its own production capacities"*[15], in the form of a passport blank.

After the electronic passports are made, they are distributed and "*personalized at the General Directorate of Passports within the Ministry of Internal Affairs*"[16], at the Single National Center for Personalization of Electronic Passports.

4. Security features of electronic passports

Electronic passports are equipped with a secure chip that contains a number of features designed to ensure a high level of security, including:
- Advanced encryption – so that information can be stored against unauthorized access;
- Biometric data – facial photograph and dactyloscopic impressions, which are used to identify the holder;
- Digital signature – to verify the authenticity and belonging of the travel document.

These security features ensure that the electronic passport is a reliable and fraud-proof document, protecting the holder's identity as well as their personal data.

The integrated chip allows border authorities and other competent entities to verify the authenticity of the passport and the identity of the holder through the data stored in the chip.

At the same time, this chip can include additional security features, such as a digital signature or cryptographic key, which increase the level of protection against cyber attacks and provide support in preventing forgery and fraudulent use of the electronic passport.

Cyberattacks on electronic passports are a major concern due to the serious consequences they can have in terms of national security, personal data privacy and traveler safety.

Examples of consequences of cyber-attacks:

a) Identity theft: a successful cyber-attack on electronic passports could lead to identity theft of the holders, allowing criminals to use personal information to fraudulently authenticate themselves or commit financial fraud.

Example: *a hacker manages to gain access to a person's personal and financial information in order to commit various frauds or crimes in that person's name. A notable incident where the personal data of around 500 million Marriott International customers was compromised, including names, addresses, phone numbers, payment details and passports*[17].

b) Data falsification: by manipulating or compromising the chip, criminals can falsify or alter stored information, including biometric data, to create forged electronic passports;

Example: *A criminal could clone information from a valid electronic passport and enter false data, such as a different facial photo or changed name, in an attempt to present themselves at the border under a false identity. This form of electronic passport forgery can*

---

[15] Online source: www.cnin.ro/pasapoarte.php, accessed on August 26, 2024

[16] Ibidem

[17] Johnson, R., Smith, K., "The Impact of Identity Theft on Victims: A Comprehensive Study", published in Journal of Criminology, 2018, pp. 112-129
See also BBC article from November 30, 2018 - Marriott hack hits 500 million Starwood guests, online source: https://www.bbc.com/news/technology-46401890, accessed on 6 August 2024

endanger national security and can be used to avoid travel restrictions or commit fraud or other crimes[18].

c) Cyber-espionage: criminal organizations might try to access sensitive information stored on the chip to obtain information about the owners or to compromise national security
Exemplu: *in 2014, a group of hackers managed to compromise the biometric identification chips of 5.6 million U.S. citizens stored in the Department of Veterans Affairs' Offices of Veterans Affairs. These hackers were able to steal citizens' fingerprints, personal information and other biometric data without them realizing it*[19].

d) Hacking techniques: cyber attacks on e-passports can involve various hacking techniques such as RFID[20] scanning, intercepting wireless communications, exploiting software or physical vulnerabilities to access or manipulate on-chip data.
Example: *phishing, malware, brute force attacks*

Electronic passports also have built-in anti-forgery features such as: holograms, watermarks, luminosity elements (which react differently to different light spectra - natural, infrared, ultraviolet, depending on the angle at which certain elements are observed), micro-text or variable optical elements to prevent fraudulent documents.

5. Risks to electronic passport Security and Personal Data Protection

Some of the most used methods of cyberattacks and that produce serious consequences in passport systems are:

5.1. Phishing[21] refers to a form of cyber-attack in which a criminal attempts to obtain sensitive information or personal data from electronic passport holders under the guise of false or fraudulent communication. Criminals may try to obtain data such as usernames, passwords, biometric information, or other personal data through emails, text messages, or links that appear to be from state institutions.
For example, a criminal may request personal details or electronic passport information through a fraudulent e-mail pretending to be a civil servant in the passport issuing service, under the pretext that an update or verification of data is required.
People could be misled into providing confidential data and information that could be used for fraudulent purposes.

5.2. Malware[22] is a cyber threat where malicious software is used to compromise the security of electronic passports and data stored on the chip.
Attackers can use malware to infect passport issuing and management systems to access confidential data/information (Example: Changes a cardholder's identity data) and biometric data of passport holders. This data and information can then be used fraudulently or to violate the security and confidentiality of personal information.

---

[18] Brown, A., Jones, M., ”*Fraudulent Use of Electronic Passports: Trends and Security Measures*”, published in International Journal of Criminology, 2020, pp. 245-262
[19] Smith, J. ”Cyber Espionage: The Case of Biometric Data Theft”, published in Journal of Cybersecurity, 2015, pp. 45-62
[20] RFID – Identitate prin frecvență Radio (Radio Frequency Identification)
[21] Online source: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-phishing, accessed on August 6, 2024 – definition taken and adapted
[22] Online source: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-malware, accessed on August 6, 2024 - definition taken and adapted

Malware can be introduced into the passport issuing and management system via infected malicious links or USB devices. Once introduced into the passport system, through malware, criminals can monitor and extract personal data, including blocking access to the data on the chip.

In order to prevent malware and protect the security of the electronic passport issuing and management system, it is necessary to update anti-virus programs and avoid downloading files or even accessing unknown/unsecure websites.

5.3. Brute force attacks[23] is a cyber-attack method where an attacker attempts to discover the passwords or cryptographic safeguards of a security system by repeatedly and systematically trying different combinations of characters or passwords.

These methods can be used to try to force access to the data stored on the electronic passport chip or the cryptographic keys used to secure personal information.

Attackers try to discover the passwords or codes needed to access or manipulate the data on the electronic passport chip using specialized software or technological devices.

To counter this method, it is important that security systems include measures to limit the number of access attempts, the implementation of complex passwords or access codes (for example: containing upper and lower case letters, numbers and distinctive characters, and the number of characters being sufficiently large) and regularly updated, respectively effective data encryption.

6. Conclusions

With the introduction of Romanian electronic passports into circulation, the chip has become an essential element, offering the possibility of storing data in secure digital format. Some of the most important data stored on the chip is also the biometric data of the holder, which provides a major support in quickly identifying fraud or attempted fraudulent use of such a travel document.

At the same time, electronic passports have undergone significant security enhancements by implementing advanced security features such as holograms, printing techniques, secure chips and other physical security features.

Romanian electronic passports have been issued according to the international standards imposed by ICAO, ensuring their compatibility and global recognition.

There is a significant security risk with regard to the security of the electronic passport issuing system as the personal data of document holders may be exposed or compromised. And for this reason, the authorities responsible for issuing e-passports need to take rigorous preventive measures to protect the system against cyber-attacks, while at the same time implementing robust security protocols and constantly updating the protection technology.

Regular testing of the passport system is crucial for identifying possible vulnerabilities, i.e. security breaches that could be exploited by potential attackers.

In other words, it is crucial that the electronic passport system is seriously addressed with regard to cyber risk and that a proactive approach is taken to ensure the integrity of the personal data of electronic passport holders.

At the same time, it is important for holders of electronic passports to be vigilant in providing data and information regarding their data or about the passport and, at the same time, not to provide or hand over the document to other suspicious persons. It is also necessary to handle the documents properly, without leaving the opportunity for this document to fall into the hands of any impostor.

---

[23] Online source: https://learn.microsoft.com/en-us/defender-for-identity/credential-access-alerts, accessed on 7 August 2024 - definition taken and adapted

Sources and bibliography

[1]. Brown, A., Jones, M., "Fraudulent Use of Electronic Passports: Trends and Security Measures", published in International Journal of Criminology, 2020.

[2]. Cornea, V., "Evoluția și implicațiile sociale ale pașaportului: de la scrisori de liberă circulație la pașapoarte de aur", published in The Scientific of Cahul State University B.P. Hașdeu: Social Scinces, no. 1(11), 2020.

[3]. Costea, S.G., Porojan, M., Sbîrlea, C., Popa, V., Regimul juridic al liberei circulații a cetățenilor români, printed at C.N. "Imprimeria națională" S.A., Bucharest 2019.

[4]. Johnson, R., Smith, K., "The Impact of Identity Theft on Victims: A Comprehensive Study", published in the Journal of Criminology, 2018.

[5]. Smith, J. "Cyber Espionage: The Case of Biometric Data Theft", published in the Journal of Cybersecurity, 2015.

[6]. Council Regulation (EC) No 2252/2004 of December 13, 2004, on security standards and biometric data in passports and travel documents issued by Member States, published in the Official Journal of the European Union no. L 385/1 of December 29, 2004, as subsequently amended and supplemented.

[7]. Law no. 146 of July 12, 2016, amending Law no. 102/1992 on the coat of arms of the country and the state seal, published in the Official Gazette no. 542 of July 19, 2016.

[8]. Law no. 248 of July 20, 2005, on the regime of free movement of Romanian citizens abroad, published in the Official Gazette no. 682 of July 29, 2005, as subsequently amended and supplemented.

[9]. Government Decision no. 46 of May 9, 2001 regarding the putting into circulation of the new types of Romanian passports, published in the Official Gazette no. 272 of May 25, 2001.

[10]. Government Decision no. 757 of December 30, 1993, on the putting into circulation of the new Romanian passports, published in the Official Gazette no. 24 of January 26, 1994.

[11]. https://www.bbc.com/news/technology-46401890

[12]. http://centenar.gov.ro/web/marea-unire/

[13]. www.cnin.ro/pasapoarte.php

[14]. https://www.icao.int/publications/Documents

[15]. https://www.govinfo.gov/content/pkg/PLAW-107publ173/pdf/PLAW-107publ173.pdf

[16]. https://www.researchgate.net/publication/341357883_Evolutia_si_implicatiile_sociale_ale_pasaportului_de_la_scrisori_de_libera_trecere_la_pasaporte_de_aur_The_evolution_and_social_implications_of_the_passport_from_the_free_passage_letters_to_golden_pa

[17]. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-malware

[18]. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-phishing

[19]. https://learn.microsoft.com/en-us/defender-for-identity/credential-access-alerts

[20]. https://pasapoarte.mai.gov.ro/wp-content/uploads/2021/03/comunicat-ZiuaPAS-2011.pdf