Volume XXII 2019
ISSUE no.1
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Environment friendly population records system using biometric data and anonymous signatures

To cite this article: N. F. Antonie, C. Răcuciu, F. Medeleanu, D. Glăvan and R. Moinescu, Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg. 112-121.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I1-015

Environment friendly population records system using biometric data and anonymous signatures

N F Antonie[1,4], C Răcuciu[2], F Medeleanu[3], D Glăvan[1] and R Moinescu[1]

[1]Faculty of Military Electronic and Information Systems, Military Technical Academy, Bulevardul George Coşbuc 81-83, Bucureşti 050141, Bucharest, Romania
[2]Department of Computer Science, Titu Maiorescu University, 22 Strada Dâmbovnicului Tineretului, Bucureşti 040441, Bucharest, Romania
[3]Ministry of Defense, Strada Izvor 3-5, Sector 5, Bucharest, Romania
[4]Author to whom any correspondence should be addressed

Abstract. The fast evolution of technology allowed our society to search for ways to increase efficiency and productivity. In some domains this increase in efficiency also lead to less waste, which in turn may lead to better environment protection. Such a domain is that of population records. One way to properly identify an individual is to keep a record of his biometric data. Unfortunately this method of identification is raising a lot of concerns regarding privacy and the protection of private data. This paper proposes a method of protecting biometric data by securing it with anonymous signatures. This will allow the use of that biometric data for identification purposes only and will not link it to individuals without their personal identification card (e.g. passport, ID card, etc.). It is the authors' belief that this method will increase the number of people to opt for biometric documents which will reduce bureaucracy and implicitly reduce the use of consumable materials thus better protecting the environment.

1. Introduction

Keeping a population record is a must in most modern societies. But as we all know population across the world has increased very much, especially in the last 50 years. And keeping records of billions of people is a very difficult task that needs proper recording and archiving methods and tools. This leads in the ever increasing use of consumable materials such as paper and everything related to paper printing and archiving. In the context of automation and due to the switch from paper to electronic records, the area of population records has drastically reduced the use of such materials. But, can it do even better? The answer, of course, is yes.

This paper proposes a method to further decrease the use of consumable materials, especially paper, by introducing a security mechanism based on anonymous signature schemes that will protect the biometric data of electronic identification cards when stored on the databases of population records. In a previous paper [9], the authors proposed a similar solution for the Romanian healthcare sector. This solution also had the collateral advantage of reducing the consumption of consumable materials.

The newest technology today to identify people is biometric identification. This technology is based on the human unique physiological characteristics. These unique physiological characteristics can be fingerprints, retina or iris patterns, palm veins, DNA (deoxyribonucleic acid), face or hand

geometry, etc., and all can uniquely identify an individual. Usually for biometric IDs, like biometric passports, the fingerprint is used to identify individuals.

But biometric data, like fingerprint, retina or DNA, is considered personal information which falls under the personal information protection rules and regulations (like GDPR). Also for this technology to work that data must be stored on the population records databases, allowing anyone who has/gets access to that data to obtain people's identity alongside their biometric data. And for that reason many people are reluctant to request the issuing of such IDs which are using biometric data.

In this respect, the solution proposed in this paper will allow the storage of biometric data on databases, without linking it to the identity of the individuals it belongs to. And in order to fulfill the purpose of the technology (i.e. identification), only when used by the owner in conjunction with his identification card (biometric ID card or passport) will positively id him or her and allow access to the requested services. And all this process can be done automatically without human intervention (see automatic passport verification gates on modern airports).

So the authors believe that by adding anonymous signatures to the population records systems, we can asure confidentiality to the biometric data stored so that the population will be more confident in the biometric identification technology.

2. Digital signatures

From a legal stand point a digital (or electronic) signature represents data in digital form that is attached or logically attached to other data, also in digital form, and which is used as a method for identification (article 4, pt. 3 of 455/2001 law of the Romanian legal code).

In a practical sense a valid digital signature offers the reader a strong reason to assume that the message or the digital document was indeed created by the individual or entity who signed it (i.e. authentication) and that the message or digital document wasn't changed or altered since the date it was signed (i.e. integrity). Moreover the signer cannot deny sending/signing the document (i.e. non-repudiation).

From a technical point of view a digital signature scheme is a mathematical scheme that uses a hash function to obtain the "footprint" of a document or message. In general terms a hash function computes a value from a set of data with variable length (i.e. the document or message) to a value from a set of data with fixed length (i.e. the "footprint") [11]. After obtaining the hash value, the scheme encrypts that footprint with the signer's private key in order to generate the final signature. Last step is to logically attach that signature to the respective document or message thus ending the signature process and generating a digitally signed document or message.

2.1. Standard digital signatures vs. anonymous digital signatures

Both standard and anonymous digital signatures are mathematical schemes used for proving authenticity and for providing non-repudiation and integrity to digital messages or documents. The main difference is that an anonymous signature hides the identity of the signer until the moment the need arises to uncover its identity.

One of the first practical implementations of a public-key crypto system is Rivest-Shamir-Adleman (or RSA for short). RSA is widely used for securing transmissions and for generating digital signatures. The security of RSA is based on the practical difficulty of factoring large prime numbers. This difficulty is also called the factoring problem [7].

Unfortunately RSA algorithm was proved to be vulnerable to many forms of attack. One of the most unusual attacks on RSA is the key extraction by using "Low-Bandwidth Acoustic Cryptanalysis", which is the extraction of the key by analyzing the sound generated by the CPU when decrypting a RSA-encrypted message. This attack was demonstrated in [8].

A newer algorithm used in digital signature schemes is ECDSA (Elliptic Curves Digital Signature Algorithm). This algorithm uses elliptic curves operations (point addition and multiplication) for encryption and decryption processes. The main advantage of ECDSA over RSA is that for the same level of security the former uses much smaller key sizes compared to the latter. For instance the same

level of security provided by a 1024 bit RSA key can be provided with a 160 bit ECDSA key, which is a great improvement over RSA.

Both RSA and ECDSA can be used as basis for an anonymous signature scheme. In fact any type of digital signature scheme can be used to construct an anonymous signature scheme.

2.2. Details on anonymous signatures

Now regarding anonymous signature schemes, they were first formalized by Yang et al. in [1]. The notion was further explored by other authors like Fischlin and Saraswat et al. in [2] and [3]. In a previous paper [9], the authors of this paper proposed a practical implementation of such signature schemes in the Romanian national health insurance system. Now the authors are proposing the implementation of anonymous signatures in the population records system.

As stated before, anonymous signature schemes are using standard digital signature schemes, but they provide the means to hide the signer's identity until it decides to prove it. So, for any message (m), signed with a signature σ, the identity of the signer is concealed till the moment the signer decides to reveal it. These types of signatures can be used in a variety of scenarios (e.g. electronic paper review systems, key exchange protocols, electronic voting systems like the one in [4] or in e-lottery systems as the implementation proposed by the authors of this paper in [10]).

Several authors proposed somewhat different anonymous signature schemes, the most common are the schemes proposed by Yang ([1], [5]) and Saraswat [3]. For this paper the authors focused on Saraswat scheme.

In general Saraswat anonymous signature scheme (figure 1), denoted Σ, can be considered as a triplet of algorithms: a key generation algorithm, denoted Gen (), the signature generation algorithm, denoted $Sig()$ and a deterministic signature verification algorithm, denoted $Vf()$ (i.e. $\Sigma = (Gen, Sig, Vf)$). The key pair generation algorithm is the one responsible for generating the key pair $(pk, sk) \leftarrow Gen()$. The signature generation algorithm will generate the signature by using the secret key sk and the message m:

$$\sigma^* = (\sigma, \tau) \rightarrow Sig(sk, m) \quad (1)$$

The token τ is the verification token used by the third algorithm of Σ, responsible with the signature verification at the end. $Vf()$ uses the public key pk, the message m, the signature σ and the verification token τ to output "true" if the signature is verified or "false" otherwise.

If the signature and message are valid and if there were no alterations since the signing moment, the following relation holds, for $(pk, sk) \leftarrow Gen()$, and for any $m \in \{0,1\}^*$:

$$Vf(pk, m, Sig(sk, m)) = true \quad (2)$$

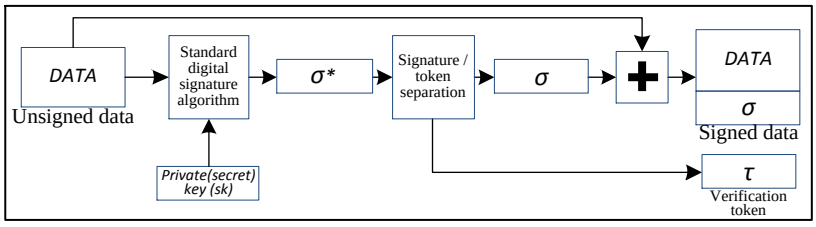

Figure 1: Saraswat signature algorithm - overview

3. Population records

Keeping a population record is a must for most modern countries today. The reasons are obvious and self-explanatory. Without such a record there will be no way to issue identification documents like passports and IDs, and without these documents there will be very difficult for a state to keep track of its citizens and to apply the laws and regulations. This can eventually lead to any sort of lawlessness and even to total anarchy. In the past this didn't happen because the number of people in the world wasn't as high as it is today (7.7 billion people as of November 2018). So now more than ever there is a need for a reliable and secure population records system. But at the same time this system has to respect basic human rights such as people's privacy.

As an example, in Romania, the population records was established in 1949, by registering all the inhabitants of the country and issuing identity documents to all Romanians aged 15 years or older.

The registration of citizens was realized by issuing personal records that constituted the local and central records. The data registered in these files being updated in a manual system, as a result of the changes occurred in the civil status of citizens, like in case of changing the home address or the release of a new identity document.

In 1990, it became necessary to modernize the population records, so that it was regulated and implemented, by switching all local manual records to electronic records (digitizing the manual paper records), by establishing the National Registry of Population Records as the main part of the National Information System for Population Records.

National Registry of Population Records is the aggregate of the personal private data of the Romanian citizens resulting from the automatic processing, in a unitary concept, in order to know the number, structure and movement of the population on the territory of the country.

It operates in an open system serving as a unique support for providing data, under the law, for all information systems that process nominal data regarding the citizens.

The two systems, manual and digital, worked in parallel until the year 2000, when manual records became an active archive for the history of the data of the Romanian citizens.

The population records system aims, on the one hand, on the knowledge of the population and its movement on different settlements, and on the other hand, the lawful communication of data and information.

Keeping population records is of great importance for the state, in the sense of knowing and individualizing all the citizens of the country, from the date of birth, of the proper development of the many relations between the state institutions and the citizens, in realizing the rights and the obligations that belong to some and to others, to monitor the movement of the population on the territory of the country and, last but not least, to support the structures of the Ministry of Internal Affairs conducting activities for preventing and fighting crimes, as well as the institutions with attributions in the field of defense, national security, order and peace public and justice.

At the same time, the identification of individuals and identity documents serve the citizens to prove their identity, their Romanian citizenship, their home address and their residence, which are necessary for the valorization of the rights and obligations stipulated in the Constitution, facilitate the various juridical relations between individuals and provide the necessary information to identify family members, other relatives, or people for whom there is not data for a long period of time.

The population records system is based on the principle of the place of residence for resident citizens and on the principle of the last home address in the country or on the last residence declared in Romania for the citizens residing abroad.

3.1. Biometric identification

The term biometry derives from two Greek words "*bios*" meaning life and "*metron*" meaning measurement. So its meaning can be the measurement of life, or more precisely of living things.

A common accepted definition of biometrics states that biometrics is the science of analyzing physical or behavioral characteristics specific to each individual in order to be able to authenticate their identity. The field of biometry itself is a branch of biology that studies living beings using statistical methods, probabilities and the principles of mathematical analysis.

So, in other words, biometric identification is the determination of the identity of an individual by using his biological, unchangeable characteristics as identifiers. Using an analogy with classical access control, instead of using a password to get access to services or resources, one can use his own biometric data to do the same.

Digitized fingerprints, hand geometry, iris or retina pattern, facial thermogram or facial pattern, voice spectrum and even the digitized handwritten signature of an individual are the most common biometrics used for biometric identification.

3.2. Biometric passport

The biometric passport (also known as an e-passport or digital passport) is an ID card usually made of a combination of paper, plastic and electronic components. The biometric data is stored on a RFID chip (Radio Frequency IDentification). This chip assures the integrity of the biometric data and the validity of the passport. The biometric standard for this type of identification card is facial recognition, fingerprint recognition and iris recognition. These were adopted after testing some other types of biometrics like retina recognition. The digital image of the biometric data is stored on the chip in a JPEG or JPEG2000 format. The comparison of the chip-stored data with the database-stored data takes place outside the passport by using an e-border system. As an oversimplification the system is made up of a passport card reader and a database as main components. The scanner reads the information stored on the passport and compares it with the information stored on the database. Afterwards it gives the ok or not ok if the data matches or not. For storing the data on the RFID chip, it uses a 32 kb EEPROM (Electrically Erasable Programmable Read-Only Memory) memory chip.

The content of the RFID chip is based on a standard developed by ICAO (International Civil Aviation Organization), ICAO Doc 9303.

Modern biometric passports systems are equipped with a set security measures in order to protect the data exchange and extraction. These measures are (among others):

- Basic access control (BAC) that allows the reading of the chip only inside the small area designated for passport reading. This measure also employs a medium-level encryption algorithm between the chip and the scanner. This measure is intended to provide protection against unauthorized reading of the passport.
- Active authentication, which is the existence of a private key stored on the passport that cannot be read or copied. This measure is employed to prevent unauthorized cloning of the passport.
- Extended access control (EAC) is the highest level of security implemented on the e-passport system. EAC employs a PKI system to secure some of the data on the passport chip. That data is encrypted with the public key of the country which issued the passport. So in order to read, alter or change that data the private key of the country of issuance is necessary.

Since the 20th of June 2009 all EU member countries must implement BAC and EAC security measures for the issuance of biometric passports.

3.3. Legal standpoint

In accordance with the provisions of European Regulation, (EC) 2252/2004 and ICAO Document 9303 Part I, Annex G, only two digital impressions are taken, saved in the database and then engraved in the electronic storage environment - respectively on the RFID chip. The general rule is to take flat fingerprints of the left and right index fingers. If those cannot be taken, the next fingers will be used. The fingerprint data is stored in NIST (National Institute of Standards and Technology) format (more precisely CBEFF - Common Biometric Exchange Formats Framework), specifying which finger was used to take the fingerprint. The facial image is taken in accordance with ICAO rules.

Due to civil liberties concerns, the digital impressions stored in the database of the population records information system are deleted automatically by an automatic procedure immediately after the electronic passport has been released or, if not released, at the latest within three months from the scheduled date of issue. Digital impressions are not centrally stored and are not intended for disclosure to third parties.

The facial image is stored in the database of the population records information system as a compressed image file. The storage term is permanent and the purpose of storing the facial image is to verify the identity of the person in the "person – data" association (in order to prevent attempts to obtain identity documents by means of identity fraud).

4. Privacy and security concerns - opposition to biometric data storage

There are a lot of groups that are opposing the introduction of biometric identification documents. Most of the concerns are related with the unknown usage of the stored data. Also there are concerns

related to civil liberties. There are also some concerns regarding the transfer between the passport and the reader. Many believe this transfer is not secure enough and wrongdoers may attempt to read the data being transferred. Some also fear that the data stored on the chip may be read by close proximity with an attacker who has the required devices to read the biometric passports. To prevent this last scenario some countries, like the USA, have implemented metallic webbings inside the passport's covers, which will act like a shield when the passport is closed.

Another issue regarding biometric documents is the data stored on the system's databases. The concern is that by storing the biometric data alongside the identity of the citizens may lead to infringements to civil liberties by the entities administering those databases. The thing that must be kept in mind is that this system is not a criminal record, it's a method used for secure and infallible identification only and the biometric data of citizens is private information. So keeping the biometric data associated with the identity of citizens is posing some concerns that are limiting the number of people opting for biometric identification cards.

As we saw in the previous chapter, from a legal standpoint, only the facial image is permanently stored in the database, not the fingerprints. This is due to civil liberties concerns. But if there was a way to securely store fingerprint data also, the system would have more ways to correctly identify individuals and to prevent identity fraud.

By introducing anonymous signatures in the method of storing the biometric data in the databases, the authors believe that the system will be able to securely store all biometric data (including fingerprint data), thus improving the identification process and reducing the amount of consumable used by the system. This might also alleviate the concerns regarding the security and privacy of biometric data, thereby increasing citizens trust in the system.

5. The proposed solution

The solution the authors are proposing for this paper is based on the introduction of an anonymous signature scheme to the population records biometric data storage method.

This process occurs before the storage of the data onto the database (just after the data was taken from the individual) and implies removing or encrypting the identification information associated with the biometric data of the individual, and signing that data with a modified Saraswat anonymous signature scheme. Afterwards the signed biometric data can be permanently stored on the database servers without compromising privacy. The verification token(s), resulted from the anonymous signing process, will be stored on the e-passport's memory chip and used anytime the owner will scan the e-passport for identification.

A step-by-step flow-chart of the signing process is illustrated in figure 2.

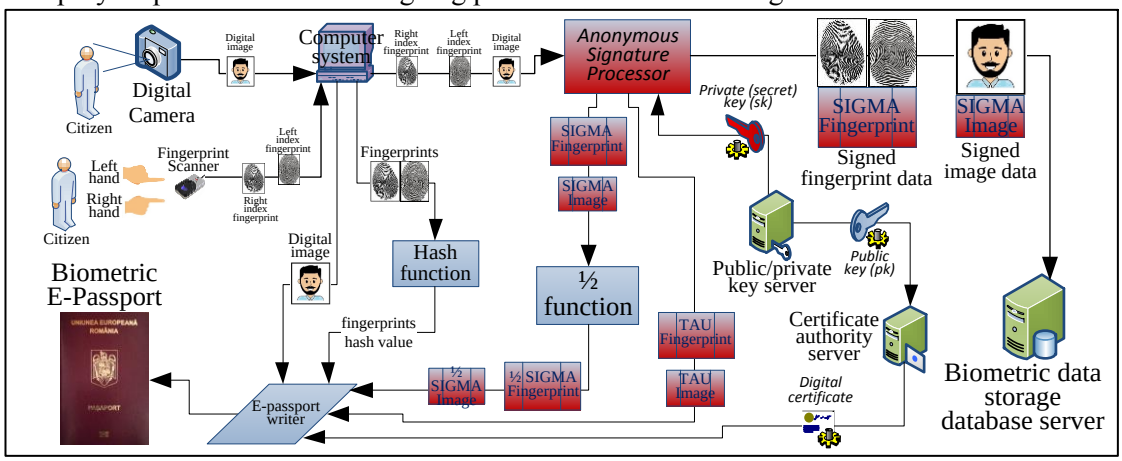

Figure 2: Anonymous signing process.

Getting into more detail, the process occurs as follows. When a citizen arrives at the governmental official e-passport issuer, he will be asked to provide the biometric data. The government worker will

take his facial image with a digital camera (denoted in the following as img) and the flat fingerprints of both left and right index fingers with a special fingerprint scanner (both denoted fgp). All these three pieces of biometric data are now in digital format and can be processed in computer systems.

Next step is to store the data in the database. To do that all identification information associated with that data will be eliminated or encrypted with the public key associated with, and unique to, that specific e-passport. Afterwards the anonymous signature can be applied to each of the biometric data taken (figure 2). For this solution the authors are proposing the use of ECDSA as a standard signature scheme on which to build the anonymous signature scheme. The reason behind this proposal is that ECDSA uses much smaller keys compared with other standard signature algorithms, yet providing the same level of security. And smaller keys means less memory on the memory chip. Thus, applying equation (1) we will obtain two Saraswat signatures (σ^*_{img} and σ^*_{fgp}), one for each piece of biometric data:

$$\begin{aligned} \sigma^*_{img} &= (\sigma_{img}, \tau_{img}) \rightarrow Sig_{ECDSA}(sk, img) \\ \sigma^*_{fgp} &= (\sigma_{fgp}, \tau_{fgp}) \rightarrow Sig_{ECDSA}(sk, fgp) \end{aligned} \tag{3}$$

where sk is the private key generated by the $Gen()$ algorithm for this specific citizen. The algorithm was described in section 2 of this paper. The actual signatures which will be attached to the biometric data and publicly released will be σ_{img} and σ_{fgp}. τ_{img} and τ_{fgp} are the verification tokens which will be kept secret on the e-passport's memory chip until the verification process.

Next problem will be to make the stored data reachable to search queries. There are several ways to accomplish this. A random number can be associated to that data and stored alongside it. That random number can even be the e-passport's number. Another way to search for the data, without the e-passport's number is to use the signature itself. But for that to work the signature, or a part of it, must also be stored on the e-passport's memory chip (which is limited).

After the biometric data has been anonymously signed, the system can store that data into its databases for later use. Being anonymously signed the data cannot be associated with individuals without the verification tokens which are kept on the e-passport's memory chip. Having that in mind, now both, anonymously signed, facial image and fingerprint data, can be permanently stored as $img||\sigma_{img}$ for the digital image and $fgp||\sigma_{fgp}$ for the fingerprint data.

To alleviate the concerns some people might have that fingerprint data can still be linked to specific individuals by associating it to the digital image data, the system is programmed to anonymously sign the facial image and the fingerprint data separately, thus eliminating the link between the two biometric data files (as seen in equation (3)). The downside is that for this to work the system must store on the e-passport's memory chip two distinct verification tokens, one for the facial image and the other for the fingerprint data.

The anonymous signature processor is described in figure 3.

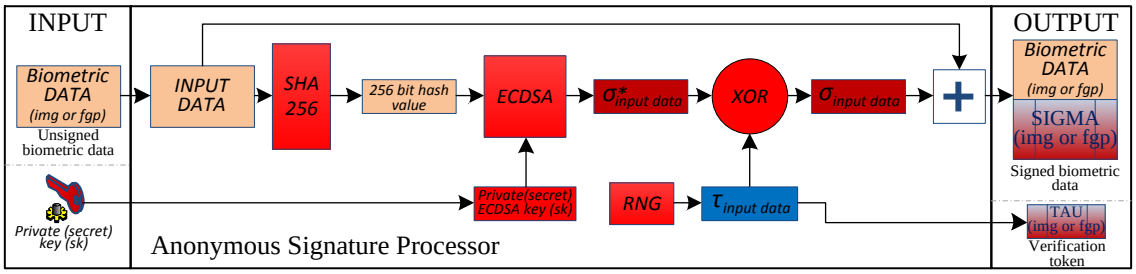

Figure 3: Anonymous signature processor - detailed flow chart.

The verification process (figure 4) allows the system to validate an e-passport by using the biometric data of its owner. In order to verify the signature the system has to first locate on the database the proper entry for this e-passport. It will do so by using one of the methods presented above (preselected random number, passport number or even the signature itself). After locating the proper entry, the signature has to be verified in order to prevent any fraud. To consider the signature verified

the verifying algorithm, $Vf()$, from equation (2) has to hold "true". Here (pk, sk) is the key pair generated by $Gen()$, which is the key generation algorithm of the standard signature scheme chosen for this anonymous signature scheme. The biometric data, img and fgp, will be verified as presented in equation (4). If the result will be "false", for either img or fgp, the signature is not valid and further investigations must be conducted under the suspicion of a false or damaged e-passport.

In order to avoid storing the fingerprints on the memory chip of the e-passport, a simple hash of that data can be stored instead. This will reduce the required space on the memory chip, but will force the system to use more computing power to also compute the hash of the fingerprint data each time this verification is invoked. But it will have the advantage to eliminate the concerns some people might have regarding the storage of their fingerprint data on the e-passports.

As shown in figure 4, when an e-passport scanner scans the e-passport, it sends to the database server the verification request containing the data needed by the database to search the specific entry. In this example that data represents half of the anonymous signatures stored on the e-passport's memory chip.

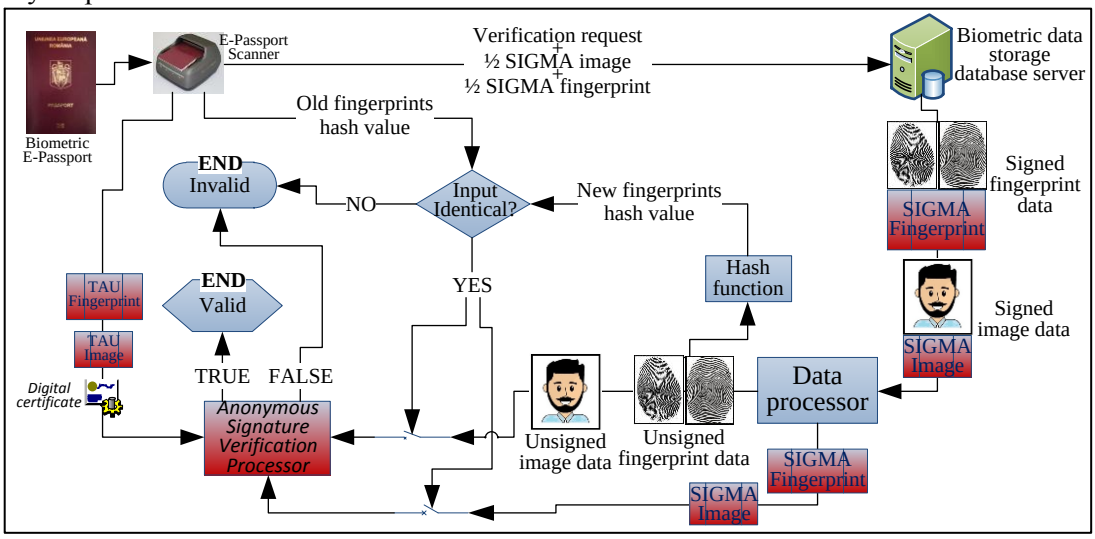

Figure 4: Anonymous verification process.

After finding the entries the database server releases the signed data ($img||\sigma_{img}$ and $fgp||\sigma_{fgp}$), which are processed by a data processor to remove the signature. Next the unsigned fingerprint's hash is computed and compared with the one stored on the e-passport's memory chip. If the hashes are identical the process can continue, if not, it will be aborted.

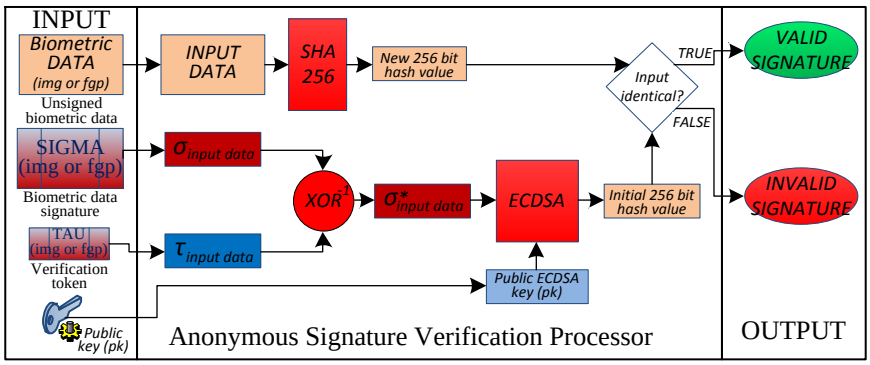

Figure 5: Anonymous signature verification processor – detailed flow chart.

Figure 5 describes the detailed operations of the anonymous signature verification processor shown in figure 4.

If the hashes are identical, all data will have to be fed as input in the anonymous signature verification processor (figure 5). The input data will be as follows: the signatures (σ_{img} and σ_{fgp}), the

unsigned biometric data (img and fgp) from the database server, the verification tokens (τ_{img} and τ_{fgp}) from the e-passport's memory chip and the public key (pk) from the digital certificate initially obtained from the certificate authority. This processor will then compute:

$$\begin{matrix} Vf(pk, img, (\sigma_{img}, \tau_{img})) \\ Vf(pk, fgp, (\sigma_{fgp}, \tau_{fgp})) \end{matrix} \quad (4)$$

If the output of equation (4) is "TRUE" for both pieces of biometric data, the verification has succeeded and the e-passport is verified thus the owner's identity is checked. If the output of (4) is "FALSE" then the verification has failed and other procedures in that regard should be initiated.

6. Security analysis and comparison with existing methods

The anonymous signature scheme proposed in this paper uses a Saraswat scheme improved with ECDSA as a base signature algorithm. The anonymous signature scheme is used to protect the privacy and confidentiality of personal biometric data in the context of newly passed rules and regulations like the GDPR (General Data Protection Regulation). The fact that the data cannot be linked with individuals permits the permanent storage of fingerprint data also.

The use of ECDSA instead of RSA will improve the security of the system by protecting against attacks like the "Low-Bandwidth Acoustic Cryptanalysis" attack, demonstrated in [8]. Another advantage of ECDSA compared to RSA is the key length, which is much smaller for the ECDSA compared with RSA and provides the same security level.

In order to alleviate concerns regarding the digital image being stored alongside the fingerprints, which may still identify individuals, the solution proposes signing both pieces of biometric data separately. This will prevent the linking of fingerprint data to digital images which can still uniquely identify individuals without having access to the individual's identification data (e.g. name, personal identification number, etc.).

Another security mechanism proposed is the storage of the fingerprints hash on the e-passport's memory chip. This will allow the verification of the fingerprint data which will abort the process if it fails. The reason for storing on the memory chip only the hash data and not the whole fingerprint data is due to privacy and practical concerns. An attacker will not be able to get the actual fingerprints even if he or she has the technology required to read the victim's e-passport. And from a practical point of view, storing only the hash of the fingerprints will minimize the required use of memory on the chip, which is limited (e.g. 32kB).

For even further security the biometric data, after being anonymously signed, can be encrypted with an asymmetric encryption algorithm, thus preventing attackers from utilizing the raw data if they manage to get access. Changing/altering the data stored on the server will be impossible because the modification of that data will result in a failure of the anonymous verification algorithm so the only thing an attacker can do if granted access, is to copy or delete the data, but not alter it.

Compared with existing methods the main advantage of implementing this solution is the use of the anonymous signatures to dissociate the identity of the people from their biometric data allowing for legally store the biometric data on permanent databases. Current deployed solutions do not allow permanent storing of fingerprint data due to legal and privacy issues. This solution solves this problem.

Another advantage of the proposed method, compared with existing ones, is the possibility to help other governmental institutions like the criminal justice institutions. For this the verification tokens can be stored also in a special database. In the case of fingerprints involved in a criminal case, a mandate can be issued to that special database to release the verification tokens for the individual who owns that fingerprint data thus identifying the respective individual. But this idea has to be very well analyzed from a legal standpoint in order not to infringe on basic individual rights.

7. Conclusions

Anonymous signature schemes differ from standard signature schemes by the fact that they can hide the identity of the signing party until the need arises to prove that identity.

This paper, like [9], proposes a practical scenario that can be improved by the implementation of anonymous signatures. The implementation utilizes modern cryptosystems like ECDSA (Elliptic Curve Digital Signature Algorithm) which further increases the security of the solution.

The solution presented here addresses the concerns some people have regarding the storage of their personal data, moreover their biometric data. But biometric data identification is one of the most precise ways to uniquely identify individuals, and its implementation can reduce the number identity thefts or similar identity crimes.

By implementing anonymous signatures, as presented here, the system can store personal biometric data without linking that data to individuals. Thus even having access to that biometric data, an attacker or a malicious person cannot determine the identity of the owner, making the data useless.

In conclusion the implementation of anonymous signature schemes allows the storage of personal biometric data, without compromising privacy, thus increasing the trust in such systems. And increasing trust in such systems means more and more people will opt to have biometric identification cards, which in turn will reduce paperwork and bureaucracy and thus further reducing the consumption of consumable materials like paper and the adjacent materials used for printing. This will lead to a better environmental footprint and a lower impact on the planet.

The authors of this paper proposed some other anonymity based scenarios, in [6] (with a revision in [10]) and in [9]. All these implementation scenarios can decrease the usage of consumable materials.

8. References

[1] Yang G, Wong D S, Deng X and Wang H 2005 Anonymous signature schemes *PKC 2006* **3958** **(**Berlin, Heidelberg: Springer) pp 347 – 63

[2] Fischlin M Anonymous signatures made easy *PKC 2007* **4450**, ed T Okamoto and X Wang **(**Berlin, Heidelberg: Springer) pp 31 – 42

[3] Saraswat V and Yun A Anonymous Signatures Revisited *ProvSec 2009* **5848**, ed J Pieprzyk and P Zhang **(**Berlin, Heidelberg: Springer) pp 140 – 53

[4] Gang C An Electronic Voting Based on Multi-Party Computation *ISCSCT '08* 10.1109/ISCSCT.2008.80 (Shanghai: IEEE)

[5] Yang G, Wong D S and Deng X Efficient anonymous roaming and its security analysis *ACNS 2005* **3531**, ed J Ioannidis et al **(**Berlin, Heidelberg: Springer) pp 334 – 49

[6] Medeleanu F, Racuciu C and Antonie N F 2017 Anonymous signature schemes applied for a fair e-lottery system *The international conference "Education and creativity for a knowledge-based society" 11th edition* ISBN 978-3-9503145-5-7 pp 32 – 7

[7] Stinson D R 1995 Cryptography: Theory and practice third edition, ed K Osen (Boca Raton: Chapman & Hall/CRC Press)

[8] Genkin D., Shamir A., Tromer E. (2014) RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Advances in Cryptology – CRYPTO 2014 **8616**, eds Garay J.A., Gennaro R. **(**Berlin, Heidelberg: Springer) pp 444 – 61

[9] Antonie N F, Răcuciu C, Glăvan D, Medeleanu F, 2018 A security mechanism based on anonymous signature schemes as a method to reduce the consumption of consumable materials, *IOP Conference Series: Earth and Environmental Science* **172**, 10.1088/1755-1315/172/1/012007, 012007

[10] Medeleanu F, Răcuciu C, Nen M, Liepe Z, Antonie N F, 2018 Fair e-lottery system proposal based on anonymous signatures, *Applied Economics incorporating Applied Financial Economics 1-13*, 10.1080/00036846.2018.1563671

[11] M. Rogobete, 2018 Hash Function and Collision Resistance, *International Conference Education and Creativity for a Knowledge Based Society, 12th Edition*, ISBN 978-3-9503145-5-7 pp 54 – 7