Bokareva, A. A. (2020). Personal authentication using verified electronic document. *Actual issues of modern science. Collection of Scientific Articles. European Scientific e-Journal*, *6* (6), *1*, 5-11. Hlučín-Bobrovníky: "Anisiia Tomanek" OSVČ.
Бокарева, А. А. (2020). Персональная аутентификация с использованием верифицируемого электронного документа. *Actual issues of modern science. Collection of Scientific Articles. European Scientific e-Journal*, *6* (6), *1*, 5-11. Hlučín-Bobrovníky: "Anisiia Tomanek" OSVČ.

DOI: 10.47451/inn2020-09-001

The paper is published in Crossref, ICI Copernicus, BASE, Academic Resource Index ResearchBib, J-Gate, ISI International Scientific Indexing, Zenodo, OpenAIRE, BASE, LORY, ADL, Mendeley, eLibrary, and WebArchive databases.

Alyona A. Bokareva, Reseacher in electronic documentary, Undergraduate, ITMO University.
St. Petersburg, Russia

Personal authentication using verified electronic document

Abstract: In the modern world, there are quite a large number of various documents that certify (both independently of each other and in aggregate) both the identity of the owner and his social and legal rights and opportunities. However, there are several problems in this field. The paper dwells on the research of the possibility of bringing personal identification documents to a digital format with guaranteed person authentication and verification of the document, based on the digitalization trends of modern society and the increasing capabilities of technical support to eliminate the likelihood of damage, falsification and other negative impacts on the existing document flow. The main problem in solving this problem is the choice of the most effective type of used biometric parameters of a person for reading, broadcasting and subsequent processing.

Keywords: authentication, electronic document management, digitalization, personal identification, biometric parameters.

Алёна А. Бокарева, исследователь в области электронной документации, магистрант,
Университет ИТМО. Санкт-Петербург, Россия.

Персональная аутентификация с использованием верифицируемого электронного документа

Аннотация: В современном мире существует довольно большое количество различных документов, которые удостоверяют (как независимо друг от друга, так и в совокупности) как личность владельца, так и его социальные и юридические права и возможности. Однако в этой области существует несколько проблем. В статье подробно рассматривается исследование возможности перевода документов, удостоверяющих личность, в цифровой формат с гарантированной аутентификацией личности и верификацией документа, исходя из тенденций цифровизации современного общества и возрастающих возможностей технической поддержки по устранению вероятности порчи, фальсификации и других негативных воздействий на существующий документооборот. Основной проблемой при решении этой задачи является выбор наиболее эффективного типа используемых биометрических параметров человека для считывания, трансляции и последующей обработки.

Ключевые слова: аутентификация, электронный документооборот, оцифровка, идентификация личности, биометрические параметры.

Introduction

In the modern world, there are quite a large number of various documents that certify (both independently of each other and in aggregate) both the identity of the owner and his social and legal rights and opportunities. However, there are several problems in this field:

- most of the documents are in the paper version, which significantly reduces the wear resistance and durability;
- an existing document can be verified for authenticity and established compliance with the identity using special tools and access to a single database, which significantly affects the speed and ability to verify, e.g., if there is no technical possibility of communication with the database;
- user authentication occurs by photo, which leads to possible errors (when changing appearance, with age changes, relatives, doubles);
- constant changes of documents (when reaching the age, changing data, adding new functions), so stored information, related to the user, grows exponentially during the life of the person;
- due to the high growth rates of innovative and digital technologies, it is necessary fully to replace current documents with electronic ones without loss of originality and security;
- due to the growing mobility of citizens, as well as to ensure the constant possibility of identity authentication, the transition to multi-copy (without loss of originality and authenticity) electronic documents is a necessity, dictated by the rhythm and quality of life and the increasing amount of information in the world requiring a certain systematization, protection, and proper storage and display with the function of a quick search of needed information.

To date, the first attempts have already been made to switch to electronic documents for citizens, but encryption methods using personal characteristics of a person are not applied for their use and security. One of these developments is the *Electronic Passport of a Citizen of the Russian Federation*. The project is a plastic card with a chip sized a bank card. In addition to the usual passport data, fingerprints, iris pattern and other biometric authentication data, driver's license data, migration registration data, *INILA* (Insurance Number of the Individual Ledger Account), *ITN* (Individual Taxpayer Number), as well as an electronic signature can be recorded on it (Electronic passport of a citizen of the Russian Federation), which is an intermediate stage between the transition to a fully electronic document format from paper media and the reduction of stored databases by reducing the number of documents.

The results of the study

The first association when discussing identity authentication using electronic documents and/or technical means is the use of biometric parameters, and this is really the simplest (in terms of the availability of parameters) and logical way to identify a person. However, when

considering in detail the possible types of biometric parameters, their reading and analysis, we can conclude that this task is not so elementary even at the stage of selecting parameters without taking into account the second part of the task, namely, the use of a verified electronic document to authenticate. So, this task is automatically divided into two subtasks:

- determining the type of biometric parameters;
- a verified electronic document containing the information necessary for identity authentication.

To solve these main problems, it is proposed to assume that there is an abstract universal system to read, analyze and process biometric parameters (and information about them in an electronic document) of any type.

We should consider the first part of the problem, namely: choosing the type of biometric parameters. The most common currently (and the oldest way: the hypothesis of the immutability of the papillary pattern of the palmar surfaces of human skin was put forward by William Herschel in 1877 and was first used to identify a criminal in the UK in 1902) is fingerprinting, otherwise, scanning fingerprints, to be more precise, the capillary pattern of the fingertips. At the moment, 100% uniqueness of each individual's fingerprints is not clearly defined, and this statement is based only on practical data (*Kukharev, 2001*). Practice shows that the fingerprints of different people may have the same global characteristics, but there are no identical micro-nodes. Therefore, global characteristics are used to divide the database into classes at the authentication stage. At the second stage of recognition, local features are already used. Upon detailed examination, it turns out that the results can be significantly distorted with a certain reading error (depending on the quality of equipment, surface cleanliness, finger cleanliness, the presence and absence of skin damage, the position of the finger on the scanner) and the use of this method in electronic document management can bring more difficulties than simplifications and optimization of the process for both the identified person and the body identifying this person. Fingerprint conformity assessment is performed using the formula:

$$K = \frac{D^2}{p * q} * 100$$

there:

D – the number of matched minutiae (local patters),

p – the number of standard minutiae,

q – the number of identifiable fingerprint minutiae.

If the result exceeds 65%, the prints are considered identical (the threshold can be changed when setting other accuracy parameters) (Dactyloscopy).

The second most popular parameter is the iris. The first discoveries in this field were made in the late 1930s. In 1936, American eye surgeon Frank Bursch was the first, who thought that the human eye and its iris can be used for personality recognition, and his idea was patented by Leonard Flom and Aran Safir in 1987. In 1989, they turned to John Daugman to develop recognition theory and algorithms. It is John Daugman who is considered to be the founder of this method of biometric authentication. Today the authentication technology using iris scanning is gaining popularity and is one of the leading information security technologies on the market (*Iris authentication*). The process of recognizing a person using the iris can be divided into three

stages: digital image acquisition, segmentation, and parameterization. The image for analysis is made in high quality. for this purpose, a monochrome *CCD-camera* with dim illumination is used, which is sensitive to infrared radiation. After defining the borders, the iris image must be normalized. After normalization using pseudo-polar coordinates, the selected area of the image becomes a rectangle, and the radius and centre of the iris are estimated (*Dmitriev et al., 2016*). The iris of the eye is considered one of the most convenient to be scanned and one of the most constant parameters during a person's life, but it can change quite significantly with severe injuries and surgical intervention.

Another of the most commonly used and easy-to-process parameters is the human voice. This method is currently widely used in banking and other structures with the possibility of voice calling. There are a sufficient number of ways to define parameters for voice identification, as well as to store data for processing and comparison with the stored template. However, in cases of colds, allergies, and other diseases that cause voice signal distortion, this system has a high risk of access failure, which significantly affects the quality of identification availability and the tasks outlined above (*Gavrilova & Taran, 2020*).

The different distribution of blood vessels in the retina of the eye has a structure that is unique to each individual, so it can be used as a means of confirming the identity and is the most reasoned for the purposes set out in this paper. Thanks to the work of Dr P. Tower, it was found that even in twins, the structure of the retina is different (*Kukharev, 2001*). The retina does not change much during a person's lifetime, except in cases of illness or blindness. In terms of scanning complexity, the retina slightly exceeds the iris but, in terms of usability of the data, obtained during scanning, the retina is the most preferable due to the possibility of a coordinate method for selecting the scanning area, the amount of information stored and evaluated, and the number of unique parameters and characteristics for comparison and identification (Authentication via the retina of the eye). Research by the US national laboratory showed that the probability of a second-type error with this authentication method is extremely low (less than 1%). Based on the analysis provided, the most preferred type of biometric parameters for identity authentication is retinal scanning.

To solve the second part of the problem, namely, determining the verified document for identity authentication, it is necessary to determine:

- parameters, which this document should have,
- the method of storing and verifying this document,
- the type of information for identity authentication.

The document identifying the bearer's identity must have comprehensive but not over-saturated data about the person. At the moment, such data is the last name, first name, patronymic (if it is), date of birth and a unique number assigned to a document (not a person) that certifies the identity and when issuing a new document (or a new type of document, such as a driver's license), a new number is assigned, so in turn, this leads to progressive amounts of stored information about each identified person. When switching to electronic document management, it is advisable to replace all existing identifiers (document numbers) with a single unique number assigned to a person but not to a specific document. For this reason, the universal data set (passport, driver's license, *INILA*, policy, etc.), in turn, must and should be replaced by a single electronic document with the social and legal characteristics of a particular person

(identified person) registered and fully integrated into a common database. This system will allow us to store simultaneously all relevant information in a single 'file', prevent the reproduction of various forms and the number of documents (and their identifying numbers that need to be stored later) increasing the risk of loss and distortion. Also, this system will provide ease of use and comfort both for the user and for various government, and other interested structures, due to the possibility to use outside the stable communication zones without carrying additional devices and forms (for the user), a high degree of reliability and speed ensuring minimal failures for the first and second types of errors.

The method of storing an electronic document must not only be reliable but also convenient for the person himself allowing to present and use the document at any time and in any conditions, even if there is no electronic device. This postulate leads to an understanding of the need to create a multi-copy protected document that can be stored not only on the original physical media but also in the cloud space with conditionally open access. This storage method imposes additional restrictions and increases the necessary degree of document protection to avoid the possibility of distortion, loss, availability, and falsification of the document.

To authenticate an individual using the proposed format of an electronic document, it is necessary to put an area in the document itself that stores information about the biometric parameters of the individual. The most correct approach, in this case, is a distributed point record of data in the entire volume of an electronic document, the storage coordinates of which will be determined using a unique encryption algorithm determined and calculated from scanned biometric data, thereby reducing the likelihood of errors when reading the document, data falsification, and the possibility of dynamic changes in the document itself and the variability of its use. Thus, biometric parameters will be not only an authentication system, storage method, and document coordinate plane but also a key for data decryption making the system as autonomous, independent, and secure as possible, accessible to identity authentication at any time without the cost of storing and accessing the person database, which in large cities and countries significantly reduces the load and saves both time and material resources not only in the short term, but also in the long term, when the system is constantly used, due to the absence of the need to re-issue any printed or other verified documents, the issuance of several types of documents per person, and the reduction of interdepartmental queries and data flows due to the availability of complete information about the person in one "file".

Conclusion

In conclusion, it should be noted that the proposed system, in contrast to existing solutions, makes it possible:

- simplify and reduce both the use of identifying documents and their number, reduce the risks of erroneous acceptance of documents, incorrect processing of citizens' applications, and then avoid pre-trial and judicial proceedings in connection with incorrect data or their processing, including falsification;
- reduce the cost of producing and printing standard types of documents on paper and other physical media in a special secure way, re-issuing and printing them if they lose or lose their readable form;
- reduce the number of documents used to one per person;

- implement a comfortable environment for using documents for their owners.

References:

Authentication via the retina of the eye. Modern Electronic Library. Moscow. (in Russian)

Dactyloscopy. Modern Electronic Library. Moscow. (in Russian)

Dmitriev, E. A., Shveikin, V. V., & Tanaev, I. V. (2016). Authentication by the iris. *Research and Development of Students: Materials of the 4th International Student Scientific and Practical Conference*, 144-147. Cheboksary: CNS Interactive Plus. (in Russian)

Electronic passport of a citizen of the Russian Federation. Modern Electronic Library. Moscow. (in Russian)

Gavrilova, A. S., & Taran, V. N. (2020). Protection of personal information using biometric data. *Colloquium-journal*, *12* (64), 43-44. (in Russian)

Iris authentication. Modern Electronic Library. Moscow. (in Russian)

Kukharev, G. A. (2001). *Biometric systems: Methods and means of identifying a person's personality*. St. Petersburg, Polytechnics. (in Russian)

Smith, R. E. (2002). *Authentication: from passwords to public keys*. Williams. (in Russian)