EU SERVICE DIRECTIVE, DIGITAL IDENTITY AND ID DOCUMENTS IN BOSNIA AND HERZEGOVINA

Sinisa Macan

Chief of Department for IT Infrastructure and Security, Ministry of Interior of Republic of Srpska, BiH

sinisa.macan@mup.vladars.net

Case study

DOI: **10.7251/JIT1801032M** UDC: **004.738.5:341.217(4-672EU)(497.6)**

Abstract: In 2006, the European Union adopted the Services Directive, which establishes the obligation to establish unique points of contact through which citizens and businesses receive certain services from government bodies. The Services Directive unifies the services market throughout the European Union and creates an obligation for each Member State to improve its way of providing services to citizens. Citizens are accessing services through digital identities.

Having in mind that Bosnia and Herzegovina have for more than 65% turnover with EU countries, there is a need and legal obligation for the introduction of the same standards in the field of digital services and digital identities in BiH as in the EU. Citizens and businesses in Bosnia and Herzegovina need to have same position with competitive and compatible markets in EU countries. To validate digital identities, it is possible to use ID documents in BiH. This paper described the way of validating the digital identity in BiH using ID card or passport. ID documents issued according to ICAO 9303 standards and EU regulations must have embedded chips. These documents can be used to access electronic services as well as for digital identity verification.

Keywords: Digital identity, ID documents, BAC, EAC, SAC, interoperability, PSCs, Service Directive.

INTRODUCTION

With the development of technologies, electronic procedures can be created in which persons with real identities appear through digital identity. Persons can be involved in the procedures accessing appropriate resources, while the Internet becomes the medium to which resources are connected and through which communication is made. Following technological development, public administrations have to adapt their business processes to make their activities more efficient and cost-effective, and open new channels of communication with citizens.

Electronic procedures contribute to the modernization of public administrations, making them more efficient. The use of electronic procedures is shown to be cost-effective, both in terms of cost and time. The European Union has defined the obligation to establish a single market and the same conditions in the EU Member States, and later on, in accordance with the "e-government" objectives, foresees the establishment of electronic procedures and services not provided for in the EU Services directive of the European Parliament and of the Council of 12 December 2006, (2006/123/EC) [5]. The principles defined in the Services Directive can therefore also be used when providing services to business entities. The European Commission has adopted two decisions to implement the Services Directive.

The first is the Decision of 2 October 2009 [1] on the establishment of practical programs for the exchange of information by electronic means between Member States in accordance with Chapter 6 of the Services Directive. In accordance with that decision, the Internal Market Information System (IMI) is used to exchange information for the purposes of

the Services Directive. The Internal Market Information System was established in accordance with Decision 2004/387/EC of the European Parliament and of the European Council of 21 April 2004 on the interoperable delivery of pan-European "e-Government" services to public administrations, businesses and citizens (IDABC) [3].

The second decision is the European Commission Decision of 16 October 2009 [7] on the establishment of measures enabling the use of electronic means by means of "points of single contact" (PSCs – Points of Single Contacts) in accordance with Directive 2006/123/EC on services in the internal market. This Decision concludes that the completion of procedures and formalities through PSCs must be possible across borders between Member States as defined in Article 8 of Directive 2006/123/EC. In order to comply with the obligation to simplify procedures and formalities and to enable cross-border use of SCPs, procedures by electronic means should rely on simple solutions, including the use of a digital signature and digital identity. It is for these purposes that they can use ID documents, which can store digital signatures. PSCs are online e-government portals that allow you to [7]:

- Find out about the rules, regulations and formalities that apply to service activities
- Complete the administrative procedures online (by submitting the necessary application forms and supporting documents etc. electronically)

All national PSCs are part of the European EUGO network.

After an appropriate risk assessment, specific procedures and documents may require an advanced digital signature, based on a qualified certificate, which is equivalent to a manual signature. Each Member State shall establish, maintain and publish, in accordance with certain technical specifications, a "confidential list" containing minimum information regarding accredited providers of certification services.

Implementation of the European Directive on Services by Member States requires the adoption of legislative and organizational measures. For the implementation of the EU Services Directive, the EU has adapted the legislation and implementing regulations in such a way that legal transactions that are conventionally made and legal transactions that are digitally made are placed at the same level. The EU Services Directive is related to the Treaty on the Functioning of the European Union [21], in particular in the part relating to the Internal Market of the European Union. Treaty relating to the establishment and functioning of the EU govern the freedom of movement and performance of the Union's entire territory. National legislation regulates service activities in accordance with Articles 49 and 56 of the Agreement on the Functioning of the EU [21]. It is imperative that public administrations must adapt their procedures so that they can provide electronic access to services through one or more access points within the country.

The purpose of the EU Services Directive is to create equal and competitive conditions throughout the Union. As Bosnia and Hercegovina has the largest turnover with the EU, it is necessary that there are similar business conditions and similar services in BiH as in the EU. Bosnia and Herzegovina has the largest share of its business exchanges with the European Union and CEFTA countries. According to the Chamber of Commerce of Bosnia and Herzegovina, from the total commodity exchange in 2016, 65.18% refers to European Union countries and 13.5% to CEFTA countries [28]. In addition, Bosnia and Herzegovina, by signing the Association Agreement (The Stabilization and Association Agreement between Bosnia and Herzegovina and the European Union was signed on 16 June 2008) [24], has undertaken to align its legislation with EU legislation. Chapter IV of the Stabilization and Association Agreement between Bosnia and Herzegovina and the European Union defines freedom of movement for goods between Bosnia and Herzegovina and the European Union and Chapter VI of this Agreement defines the obligation to harmonize legislation in Bosnia and Herzegovina with European Union (Article 70 paragraph (1) of the Stabilization and Association Agreement between Bosnia and Herzegovina and the European Union reads as follows: "1. The Parties acknowledge the importance of harmonizing existing legislation of Bosnia and Herzegovina with EU legislation and its efficient implementation. Bosnia and Herzegovina will seek to ensure the gradual alignment of its existing laws and future acquis with the acquis. Bosnia and Herzegovina will

ensure proper implementation and implementation of existing and future legislation.)[24]

In order to provide access to electronic services provided by a public administration, it is necessary to identify person who ask some service from public administration. The service can be accessed via the Internet, and the person must be efficiently authenticated and reliably validate his real identity through digital identity.

In this paper, the main issues of digital identity in Bosnia and Herzegovina are presented. The analogy between the real and digital identity is established, and the concept of identity management is described. Furthermore, an identity-based identification concept based on the ICAO 9303 document was presented through an electronic document. Finally, based on the ICAO 9303 document, a document ID system was established in Bosnia and Herzegovina and the content of the BiH electronic ID card was presented, which can be used as a means of validating the digital identity in Bosnia and Herzegovina.

The Notion of Identity

Identity is a set of all known personally identifiable information. The number of this data can be extremely high. This is birth data, names and surnames, relatives, physical characteristics, preferences, profession and education, social status, health, and a complete set of characteristics that identifies a person. However, one part of a data set to a person can uniquely identify such a person, or make his authentication. A person appears, we know his identity by name and surname, and the competent state authority through the identification procedures confirms that this really is that person. Such a person has access to certain jobs or education or social protection system or other resources available in the real world [20].

People in real life access resources. For some more important resources, they must have special access permissions, which are obtained on the basis of appropriate certificates issued by other entities from the real world. Such entities can be organizations or individuals. For driving a car, it is necessary to identify the person and to know his identity that he knows how to operate the car in order to enable him to use such a resource. If he or she does not possess the knowledge to manage such a resource, it can cause a breach of security and a violation of the rights to the health and life of others. Confirmation that a person of a particular identity can manage the vehicle's resource is reissued by the state authority.

The real identity model consists of the following terms [22]:

1. A person with certain characteristics has a certain identity
2. Identity is a set of data about your face, such as its properties, preferences and features
3. Characteristics are information about the person who determines it, such as name, surname, date of birth, health data, and data acquired through education, skills and the like
4. Preferences are information about a person that characterizes the person's habits
5. Characteristics are data that the person inherits, such as hair color, eyes or biometric data
6. A resource in a real world is a property or a right or a public good for which a person may have an interest
7. A person confirms his information with specific evidence of his identity issued by an authorized body, such proof is in real life an identity card or identification document
8. Identification information is on the given identity certificate
9. The authentication procedure determines whether a person with a certain identity has the right to access the appropriate resources

The above text explains the notion of identity and the way of identifying a person in the real world. The Internet is a global information and communication system that contains many sets of digital data, that is, logical resources that can be accessed from the real world through access devices. As data, as logical resources, does not have a conventional physical reality, this digital world within the Internet is also called a virtual world. Data sets on the Internet are models of real or abstract objects in a computer-readable form. A special case of a model of a real world object is a model of a citizen. Each model, and so on, the citizen model, in order to be practically usable, it should be authentic to the original to the extent that it descriptively contains the user requirements.

In the real world, state authorities establish citizens' registers, and issue personal documents that

serve to authenticate citizens. In the case of a citizen register, user requests arise from the relevant national and accepted international normative solutions in the domain of law. If a set of citizen model data sets is sufficient to establish a mutually unambiguous correspondence between a citizen and an appropriate subgroup of citizen data in a computer readable form on a request, we will say that this subset of data represents the digital identity of citizens. For the real functioning of the real and virtual world, it is necessary to establish a system of trust between the entities from the real and the digital world, that is, to establish mechanisms for the confirmation of access to resources from the digital world.

The digital identity of a citizen can be used in many ways. For an example, it can be the basis for managing the right of access to physical or logical resources within a computer or communication system. Today, there are several global systems for this purpose and are known under the common name of identity management systems (the US National Institute of Standards and Technology - NIST working with the Department of Commerce has defined one of the systems for managing identities. Of particular security interest are identity management systems at border crossings, such as the Schengen Information System (SIS) [6].

Digital Identity and Internet

The Internet, with all the computers connected to the Internet, contains a real-world model in which digital resources are stored and exchanged with resources, that is, information available under certain rules [23].

In the business world, especially in the banking sector, the concept of user identification has been established in order to conduct banking transactions. A large number of companies issue special cards for accessing resources and conducting business activities.

In accordance with the needs, Identity Management has been developed. In a digital environment that, via Internet technologies, is expanding to a global digital environment, a certain entity through communication channels provides a set of information about itself. The set of information available is changed depending on the context. Identity management allows a person to use an exact digital identity at a given time, for the purpose that he needs, the relationship is used in the right context at the right time. Identity management is viewed as a concept for [20]:

- defining the actual identity of the person represented,
- keeping relevant information about the entity, or a person in a safe and flexible manner,
- providing access to information in a well-defined manner in an adequate environment,
- the establishment of a flexible, distributed and high-quality identity management infrastructure.

In order to realize the concept of digital identity management, it is necessary, through appropriate steps, to authenticate the person, or to present it. A person or entity may be represented, for example, in the following ways:[8]

- something that the person knows (username and password)
- something that a person has (a corresponding token or card)
- something that the person possesses and knows (identification card)
- something that the face is (biometric data)
- something that a person is and what he knows (biometric data with a credit card with an identification code.

Once a person is presented or authenticated, then the authorization process, that is, confirming the allegations from the authentication process and approving access to resources, is initiated.

It is possible to introduce an access control mechanism when determining whether a person really has the right to access certain resources. The monitoring mechanism involves determining whether all identity management processes are adequate [15].

The concept of a digital identity is a real-world identity model. In the real world, each individual is identified by registering himself, giving his name, surname, and other attributes that make him unique. Institutions of trust, which perform the act of registering a person, are the authorities of the state. These authorities shall issue appropriate documents to persons, as a kind of evidence of the person's identity. On the basis of these documents the right of movement and freedom is allowed.

One person can have a larger number of digital identities. As a large number of social activities, including business, take place through the Internet, there is a need for standardizing the process of creating a digital identity, and modeling a digital identity with a real identity.

In the real world, personal identification documents are issued. Personal documents have evolved into electronic personal documents in the last ten years, that is, standards have been created that enable the issuance of personal documents with a built-in chip, which contains stored data that can be used for identification purposes in the digital world.

ICAO System of Documents

Freedom of movement, and the right to personal safety and security and the right to nationality and the choice of a home where a person is to live are guaranteed by international documents. Documents adopted by the United Nations are incorporated into the constitutions of the UN member states. Also, the documents adopted by the Council of Europe and the European Union guarantee the rights to freedom of movement, and the right to citizenship, security and personal freedom [6].

Through the evolution of legal regulations guaranteeing fundamental freedom and human rights, control mechanisms have been developed, as well as mechanisms for implementing certain guaranteed rights. With the development of technologies and the development of traffic in the twentieth century, the need for a man to travel and change the place of residence and work has been increasingly expressed. Globalization completely changes the needs of man, and the jobs that a person performs. Also, the needs of man change, and the need for travel between countries and continents is extremely evident. A modern man travels for work, for learning, for curiosity and for tourism. There is an extremely intensive traffic between countries and continents.

The most common way of transport is by plane. At the beginning of the second decade of the twenty-first century, approximately 2.8 billion passengers were transported on airplanes [25], which is about 7.5 million passengers per day.

At airports it is necessary to provide a complete infrastructure that ensures fast flow of passengers, but also a safe border crossing. The United Nations legal framework, which is translated into regional and national legislation, guarantees the right to freedom of movement, but also the right to a safe environment and personal freedom. The data indicate that the largest number of passengers between countries, but also between continents, uses air traffic. Border crossings have been established at airports. Crossing the border should be quick in terms of a guarantee of the right to freedom of movement, but at the same time it should guarantee the right to a safe environment, or to reduce the risk of passing passengers that could endanger the safety of others.

The United Nations International Civilian Aviation Organization (ICAO) creates standards for identification documents that are implemented in Member States and which should facilitate border crossings, and improve controls and reduce the risk of unwanted border crossings. Thus, ICAO defines standards for ID documents (ICAO - International Civil Aviation Organization) in ICAO 9303 document [26]. Members of the ICAO are 191 countries.

The intensive development of technical possibilities related to the system of documents created the need for continuous improvement of recommendations and standards. The current valid ICAO document 9303 includes the following group of documents [26]:

1. Part 1: Introductory document, seventh edition from 2015 - introductory part containing general data, links to other standards, descriptions of concepts and structure of document 9303.
2. Part 2: Safety Specifications for Design, Production and Issue of Machine-Readable Documents, Seventh Edition of 2015 - defines mandatory and optional specifications and prerequisites that must be met by the competent ICAO Member States issuing documents to ensure the process of issuing and personalizing personal documents, the protection of the rights of the document holders, and the measures taken to reduce the risk of forgeries of documents. Mandatory and optional specifications for the physical protection of the document itself, and the premises where the documents are produced and personalized, and recommendations for officers working on

procedures related to document identification documents.

3. Part 3: Common specifications for all machine readable documents, seventh edition of 2015 - define common specifications for travel documents of different dimensions. Namely, according to the ICAO specification or ISO (International Organization for Standardization) international standardization standards, travel documents are divided into four basic sizes: Travel Document 1 (TD1) (ID card), TD2 (standard size for visas that are admired in passports), TD3 (passport size).
4. Part 4: Specifications for machine readable passports and other machine-readable travel documents of size 3 type, seventh edition of 2015 - describes the technical specifications for passports or TD3 documents, according to the International Organization for Standards (ISO). The focus is on physical and optical elements of protection.
5. Part 5: Specifications for other type 1 travel documents, seventh edition of 2015 - describes the technical specifications for TD1 size documents, according to the ISO size of the ID card.
6. Part 6: Specifications for other type-2 travel documents, seventh edition of 2015 - technical specifications of the size of TD2, according to ISO.
7. Part 7: Machine-readable visas, the seventh edition of 2015 - describes the technical characteristics for visas.
8. Part 8: Reserved for emergency travel documents, which should be described in the following period.
9. Part 9: The development of biometric identifiers and data warehouses in electronic machine readable documents, seventh edition of 2015 - describes the electronic memory elements contained in the documents and allow Member States to put data into electronic parts of a document, and that such data is read by other countries, which guarantees global interoperability, or the ability to keep the documents legible at every place with equipment that meets the standards adopted.
10. Part 10: Logical data structure for the storage of biometric and other data in contactless chips, the seventh edition of 2015 - provides a data structure that is written in documents such that it is possible to read data according to standard devices.
11. Part 11: Mechanical protection for machine readable documents, seventh edition of 2015 - describes cryptographic mechanisms for the protection of electronic machine readable documents
12. Part 12: PKI for machine readable documents, seventh edition of 2015 - standards for data protection that are entered into electronic documents, issuing digital certificates and reading certificates in order to access data on documents.

The ICAO document system created recommendations for Member States in the domain of citizen identity management. Citizens' identity management has a legal basis in international conventions, which are incorporated in the legislation of member states of international organizations. Through the document standardization process, efficient and fast flow of people at border crossings is ensured, guaranteeing data exchange that reduces the risk that persons who have or need to have restricted movement for safety reasons cross the border[13].

With an electronic identity, the ICAO document recognizes the media in which data models on the identity of the actual data carrier are stored [12]. The data stored in this way is used when crossing the border and a complete system is developed which allows control mechanisms in cases of identity abuse. Biometric data can be used for authentication.

The concept used by ICAO has been extended to other types of identification documents. The development of a system of documents in the world, especially in the European Union, opened projects for the establishment of a European ID card. The European ID card model was developed by the German Institute for Standardization [4], and some countries have begun to build a similar identification model, such as Hungary, and Bosnia and Herzegovina.

The concept of establishing an Electronic ID card is based on the expansion of the ICAO identity model used on passports for several new applications installed on chips [4]. On the ID card, the ICAO applet

is installed, as well as the digital presentation appliance and the digital signature applet.

On this concept it is possible to establish mechanisms that guarantee that a person in the digital world identifies the same way and the same means through which the identification in the real world takes place.

DIGITAL IDENTITY IN BOSNIA AND HERZEGOVINA

In the real world, an identity card is used to authenticate an individual. Given the existence of global standards that prescribe elements of an electronic ID, the ID card appears as an optimum option for the storage of digital identity data.

In the personal documents of Bosnia and Herzegovina, according to the law, contactless memory elements, or chips, are integrated. In Article 6, paragraphs (5) and (6) of the Law on Identity Card of Citizens of Bosnia and Herzegovina reads [17]: "The ID card form contains an electronic memory element, in which all visible data on the ID card is entered, as well as other data provided by this Law, which the Agency issues a special instruction. A citizen of Bosnia and Herzegovina may be issued an ID card containing a qualified certificate from the Agency as a competent authority. The qualified certificate contains the data prescribed by the Law on Electronic Signature of Bosnia and Herzegovina [18] and the regulations adopted on the basis of that Law. The Law on the Agency for Identification Documents, Records and the Data Exchange of Bosnia and Herzegovina [19] defines that this Agency is a certification body for issuing digital certificates through personal documents.

A contactless chip is integrated into the body of the ID card form in Bosnia and Herzegovina. The chip manufacturer is NXP [9]. The chip design is Smart MX P5CDO81A6 J3A081GA6 / T1AG2331 (mifare) for ID cards (Instructions on the contents of the electronic memory element of the identity card of citizens of Bosnia and Herzegovina [11]). A similar chip is also used for travel documents by citizens of Bosnia and Herzegovina. The chip, built into the body of the ID card, supports cryptographic algorithms (cryptography of elliptic curves) and enables a number of advanced features of the ID card.

The contactless chip communicates with the appropriate reader (terminal), which is simultaneously a read and write device. The communication of these two components is in accordance with ISO 144443 and is based on ISO 7816.

Applications on the ID card were made in accordance with the profile defined by the "European Citizen Card" standard (Part IV) [4]. The documents adopted by Bosnia and Herzegovina defining the use of this model are the Instructions on the Contents of the Electronic Memory Element of the Identity Card of the Citizens of Bosnia and Herzegovina [10].

In order for communication between the chip and the reader to be secure, cryptographic authentication methods are used (defined in the Instruction on the contents of the electronic memory element of the identity card of citizens of Bosnia and Herzegovina) [9] and [2]:

- BAC – "Basic Access Control"
- PACE - "Password Authenticated Connection Establishment"
- TA - "Terminal Authentication"
- PA - "Passive Authentication"
- CA - "Chip Authentication"

Access to the data written in the applications is possible after a successful presentation of the reader using the Basic Access Control (BAC), the authentication chip (CA), and the authentication terminal (TA) or the password protected secure connection (PACE), terminal authentication (TA) or authentication chip (CA) .

The data on the chip are organized through three applications [2]:

- biometric application
- digital representation application
- a digital signature application with a qualified certificate

The biometric application has been developed according to ICAO recommendations for travel documents so that the ID card can be used as a travel document. Based on the data from the machine readable zone, this application is accessed and identification of the identity card holder is enabled.

The digital representation application enables the holder of an identification document to present itself to a third party. When downloading an ID card, the citizen will receive a special form on which the activation code is located. Personal identification code can be for digital representation. Digital representation can be used when sending requests

for electronic services. Personal identification cod confirms the identity of the person requesting the service. Digital representation does not have the legal power of digital signing and is analogous to the physical signature given in certain cases (filing a request for a service)

The digital signature application is used to generate a qualified digital signature in accordance with the regulations used in Bosnia and Herzegovina. In order to use this application, it is necessary to implement the legal procedure and to conclude a contract between the signer and the citizen. Before using this application, it is necessary for the card owner to create a pair of keys for digital signing.

Data Access Passwords

For the needs of the BAC / PACE protocol, different passwords are used depending on the type of data access application:

- 6 characters from the first row of the machine-readable zone (16-24 characters) starting behind the "CAN" mark,
- the value of the serial number of the document, the date of birth and expiration date from the machine readable zone,
- The eID PIN is either the 5th digit transport key delivered to the owner at the time of the submission of the request or the operational 6th digit number known only to the cardholder and
- The 10-digit PUK is delivered to the owner at the time of submitting the request

„CAN" – Card Access Number

CAN is a six-digit number entered in the first line of the machine-readable zone in positions after the "CAN" mark. These are signs 19 to 24. This is a space in the MRZ for the purpose of registering arbitrary data. The password is used for BAC / PACE. This password can not be calculated based on the visible data from the ID card. It is used to establish a secure channel between the card and the terminal in cases when no entry is required from the cardholder:

- checks within the Agency for Identification Documents, Records and Data Exchange for the implementation of the Law on the Identity Card
- administrative operations at the competent authority issuing the card
- establishing a connection with a digital signature application

This password does not have an unsuccessful attempt counter. It is also used when entering EID Pina after two failed attempts.

Password from Machine Readable Zone - MRZ

Inspection systems can use a password from the MRZ instead of the CAN password for the BAC / PACE protocol. The MRZ password is in fact the SHA-1 hash value of the document number, date of birth and expiration date of the document. In this way, the existing inspection systems may use an electronic ID card instead of a passport to control the crossing of the state border. It should be noted that a certain adjustment of the software for reading the passport is needed since the MRZ's personal ID card is on the back of the document and consists of three lines (as opposed to a passport where the MRZ consists of two lines).

eID PIN

The six-digit eID PIN is a decimal number known only to the cardholder. It is used to unlock the card or access permission. Knowing this number connects the cardholder to the card. In the terminology of two-phase authentication, a personal card (card) is something "a citizen has" and an eID PIN number is something "a citizen knows."

During the submission of the request for the issuance of an eID, a transport key is generated. The transport key is used only to change that start key and generate a new permanent and only the card holder of the known eID PIN number. The use of applications installed on eID is not possible until the transport key is changed.

The chip contains an attempt counter that increases after every unsuccessful eID PIN entry. In order to avoid card locking by denial of service (DoS) during the third PIN entry, it is necessary to first enter the PUK. If the third PIN is incorrect, the card is blocked.

The eID PIN can be changed only in the way that a citizen uses the application (middleware) to enter the first existing PIN and then the new PIN.

PIN for digital signing

The chip also contains the PIN number used for digital signing. The chip provides a PIN check service that the user has entered so that the PIN never leaves the card. The chip counts unsuccessful PIN code entries and blocks the application after a third unsuccessful attempt.

The signing PIN can be changed only in the way that a citizen uses the application (MW) to enter the first existing PIN and then the new PIN.

At the moment of personalization, this PIN is not known and the user determines it at the time of generating a pair of keys used for digital signing.

PUK - Pin Unblocking Key

Once the card is blocked, unblocking it is possible using the 10-digit PUK number. The chip takes into account the number of cards unblocking. Maximum 10 unblocking is allowed. PUK is a randomly generated number that is delivered to a citizen at the time of submitting a request for issuing an ID card.

Applications that are placed on personal documents of citizens of Bosnia and Herzegovina enable digital representation of citizens, that is, the full affirmation of digital identity.

In order to access data on the chip, it is necessary to go through the steps in Table 1[27].

Table 1. *Access to data on the chip*

Chip	Terminal
	Reading EF.CardAcces
	Reading PACE passwords
	PACE
	Send chain certificate for TA TA
	Reading EF.CardSecurity
	PA (Passive Authentication)
	CA (Chip Authenitcation)
	Optional validation of the document Optional reading token for recall
	Check in tokens list (possible only for valid documents)
	Reading ED.SOD (only for the inspection terminal)
	Checking the signature EF.SOD (Passive Authentication, only for the inspection terminal)
	Select the desired application Optional read data for which terminal has access rights Calling Special Functions
	Comparison of the value of the groups of data with the values recorded in the EF.SOD file (for the inspection system only)

Electronic ID cards in Bosnia and Herzegovina are issued as of 1 March 2012, while passports are issued as of October 15, 2009 [14]. Over seventy percent of citizens of Bosnia and Herzegovina have electronic personal documents.

CONCLUSION

The paper describes the notion of identity and digital identity, with a special emphasis on the protection of identity on the Internet. The ID of the document created according to ICAO recommendations can be used for digital representation. In Bosnia and Herzegovina, a document ID is issued according to ICAO recommendations that can be used to confirm the digital identity[16]. Methods of data protection in the documents of Bosnia and Herzegovina have been presented.

In Bosnia and Herzegovina there is a developed legal and technical framework that enables the issuance of electronic identification documents. ID cards and passports of Bosnia and Herzegovina citizens own chips in which data on holders of these documents is stored. These are contactless chips that allow data to be read at a distance with the possession of adequate devices. The specificity of the BiH ID documents system is that electronic data is processed through a single technical system. Passports and ID cards have similar chips, and both documents can be used to confirm the digital identity.

On the chips in the documents there are applications for digital representation and for digital signing. Since most citizens have such documents, there is a huge potential for providing electronic services. The use of such IDs is possible in Bosnia and Herzegovina for the implementation of the EU Services Directive. In this way, it is possible to create services for citizens and business, and authentication of users by ID card. Also, it is possible to install qualified digital signatures on chip in ID cards or passports.

However, there are no software products based on electronic personal documents on the market. Also, there is no developed reader market that would allow the provision of such services. In the future, the possibility of using ID documents in Bosnia and Herzegovina for the needs of business via the Internet and confirmation of digital identity should be explored. The possibility of developing software products based on ID documents can be explored in future.

References

[1] Commission Decision 2009/739/EC of 2 of October 2009, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0739&from=EN. (n.d.).

[2] Cvijanović, Đ. (2013). Implementation of security elements of the basic control of access to electronic documents, specialist work. Banja Luka: Faculty of Information Technologies, Apeiron.

[3] Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), eur-lex.europa.eu/legal-content/EN/TXT/PDF. (n.d.).

[4] DIN. (2012). Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card Issuance, Operation and Use. DIN CEN/TS 15480-4: 2012-6 (E).

[5] Directive 2006/123/EC of the European Parliament and of the Council, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0123&from=EN. (n.d.).

[6] ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en. (n.d.).

[7] European Commission Decision 2009/767/EC of 16 October 2009, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0767&from=EN. (n.d.).

[8] Group of Authors. (2008). Network World Executive Guide for Identity management. USA: Packet Motion.

[9] IDDEEA. (2013). Architecture of Electronic Identity Cards of Bosnia and Herzegovina, Version 1.3. Banja Luka: IDDEEA.

[10] IDDEEA. (2013). Contents of the Electronic Memory Element of the Identity Card of the Citizens of Bosnia and Herzegovina. Banja Luka: Official Gazette of Bosnia and Herzegovina No. 8/13.

[11] IDDEEA. (2013). Instructions on the contents of the electronic memory element of the identity card of citizens of Bosnia and Herzegovina. Banja Luka: Official Gazette of Bosnia and Herzegovina No. 8/13.

[12] Macan, S. (2006). Specificity of design of information systems for identification of citizens, master thesis. Belgrade: FON.

[13] Macan, S., & Nogo, S. (2012). Use of biometric data and their mutual exchange in ID systems in BIH, Vol.11. Jahorina: Infoteh.

[14] Ministry of Civilian Affairs. (2002). Rulebook on the application form for issuing and replacing the ID card, the procedure for issuing and replacing the ID card and the manner of keeping records of requests. Sarajevo: Official Gazette of Bosnia and Herzegovina No. 39/02, 2 / 09,102 / 12, 41/14.

[15] Nash, A.: PKI – Implementing and Managing E-Security. (2001). Berkeley, California, USA: RSA Press.

[16] Nogo, S., & Macan, S. (2009). eServices Platform. Beograd: SMART eGovernment 2009.

[17] Parliamentary Assembly of Bosnia and Herzegovina. (2001). Law on Identity Card of Citizens of Bosnia and Herzegovina. Sarajevo: "Official Gazette of Bosnia and Herzegovina", No. 32/01, 16/02, 32/07, 53/07, 56/08, 18/12.

[18] Parliamentary Assembly of Bosnia and Herzegovina. (2006). Law on Electronic Signature of Bosnia and Herzegovina. Sarajevo: Official Gazette of Bosnia and Herzegovina No. 91/06.

[19] Parliamentary Assembly of Bosnia and Herzegovina. (2008). Agency for Identification Documents, Records and the Data Exchange of Bosnia and Herzegovina. Sarajevo: Official Gazette of Bosnia and Herzegovina No. 56/08.

[20] Sinisa, M. (2018). Registers for Identification of Citizens, Protecting of Human Rights and Efficient Public Administration. Banja Luka: Disertation.

[21] Treaty on the functioning of the European Union, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E&from=EN. (n.d.).

[22] Vasković, V. D. (2008). Application of biometric identification methods in banks, UDK 336.71:57.087. Belgrade: Association of Serbian Banks.

[23] Windley, P. J. (2003). Understanding Digital Identity Managament. The Windley Group.

[24] www.dei.gov.ba. (n.d.).

[25] www.iata.org. (n.d.).

[26] www.icao.int. (n.d.).

[27] www.iddeea.gov.ba. (n.d.).

[28] www.mvteo.gov.ba. (n.d.).

Submitted: November 17, 2017
Accepted: May 25, 2018

For citation

Macan Siniša, Digital identity and ID documents in Bosnia and Herzegovina, *JITA – Journal of Information Technology and Applications*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 8(2018) 1:32-41, (UDC: 004.738.5:341.217(4-672EU)(497.6)), (DOI: 10.7251/ JIT1801033M), Volume 8, Number 1, Banja Luka, june 2018 (1-44), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004