

MUTUAL RECOGNITION OF ELECTRONIC IDENTIFICATION MEANS UNDER THE EIDAS REGULATION AND ITS APPLICATION ISSUES

^aJOZEF ANDRAŠKO

*Comenius University in Bratislava, Faculty of Law,
Šafárikovo nám. č. 6, 810 00 Bratislava, Slovak Republic
email: "jozef.andrasko@flaw.uniba.sk"*

Abstract: The author deals with the issue of mutual recognition of electronic identification means under the eIDAS Regulation which is intended to ensure cross-border identification and authentication to online services offered by Member States. The author also reveals whether the legal order of the Slovak Republic reflects the changes that have occurred in the field of electronic identification and authentication and whether it creates a sufficient legal environment for potential foreign users of Slovak public administration electronic services.

Keywords: eIDAS Regulation, electronic identification means, identification, authentication, assurance levels, public online services.

1 Introduction

The adoption of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter referred to as the "eIDAS Regulation") represents new legislation concerning identification and authentication of persons in cyberspace of the European Union.¹ The eIDAS Regulation is directly binding and enforceable in the territory of the Slovak Republic as well as in other Member States of the European Union (hereinafter referred to as the "Member State"). Therefore, the implementation in the Slovak legal system is not necessary. However, it should be noted that from 1 July 2016, the eIDAS Regulation will only apply to the extent of trust services (electronic signature, electronic seal, electronic time stamp, etc.). With respect to the provisions governing the mutual recognition of electronic identification means, it should be noted that the obligation in question will only come into effect on 29 September 2018.² The aim of the eIDAS Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.³

2 Mutual recognition of electronic identification means – fundamental terms

In order to understand the concept and the process of the mutual recognition of electronic identification means, it is necessary to clarify fundamental terms relating to such a concept.

Pursuant to Article 3 (4) of the eIDAS Regulation, electronic identification scheme means a "system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons." Conditions to be met by the electronic identification scheme are stated in Article 6 (1) of the eIDAS Regulation. The electronic identification scheme is closely connected with the electronic identification means but this concept needs to be seen in a wider context. The electronic identification scheme provides two services, which are:

- a) issuance of electronic identification means,
- b) securing the authentication process.

Pursuant to Article 3 (2) of the eIDAS Regulation, electronic identification means is defined as "material and/or immaterial unit containing person identification data and which is used for authentication for an online service." The purpose of the electronic identification means is the authentication of person to use the online service in another Member State. It is, for example, electronic data from personal and travel documents, certificates, lists of cancelled certificates, etc. On the most general level, it is an electronic identity card. However, the purpose of the eIDAS Regulation is not to recognize electronic identity card as such but to recognize the electronic identity contained therein.

The eIDAS Regulation also defines electronic identification. Pursuant to Article 3 (1) of the eIDAS Regulation, electronic identification means "the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person." In the light of aforementioned, it is possible to identify following entities under the eIDAS Regulation:

- a) natural persons,
- b) legal persons,
- c) natural persons representing a legal person.

Person identification data are defined as a "set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established."⁴ The minimum data set for a natural person shall contain under the Commission implementing regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of the eIDAS Regulation all of the following mandatory attributes:

- a) current family name(s),
- b) current first name(s),
- c) date of birth,
- d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

In addition to the above attributes, the minimum data set must contain one or more of the following additional attributes:

- a) first name(s) and family name(s) at birth,
- b) place of birth,
- c) current address,
- d) gender.

The eIDAS Regulation also defines authentication. Pursuant to Article 3 (5) of the eIDAS Regulation, authentication means "an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed." In that regard, it is ensured that within identity proving of person and his authentication to online services are used unmodified data with confirmed integrity. Furthermore, it is ensured that such a data is the same as the data set stored on the electronic identification means. In other words, no one has changed information in the process of transmission through information systems.

Assurance levels characterize the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (e.g. identity proofing and verification, and authentication), management activities (e.g. the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. Pursuant to the

¹ Identification (declaration of identity) and authentication (confirmation of the declared identity). More on the issue of identification and authentication in: ANDRAŠKO J.: *Electronic identification and authentication in the context of electronic public administration services*. In CER Comparative European research, 2016, Iss. 2, p. 75-78.

² Article 52 (1) (c) of the eIDAS Regulation.

³ The eIDAS Regulation created a cross-border authentication system based on nodes. Pursuant to Article 2 (1) of Commission implementing regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of the eIDAS Regulation is node defined as "a connection point which is part of the electronic identification interoperability architecture and is involved in cross-border authentication of persons and which has the capability to recognise and process or forward transmissions to other nodes by enabling the national electronic identification infrastructure of one Member State to interface with national electronic identification infrastructures of other Member States."

⁴ Article 3 (3) of the eIDAS Regulation.

eIDAS Regulation, three types of assurance level are defined, in particular:

- a) assurance level low,
- b) assurance level substantial,
- c) assurance level high.⁵

3 Mutual recognition of electronic identification means – conditions

When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognized in the first Member State for the purposes of cross-border authentication for that service online, provided that the following three conditions are met.⁶

3.1 The first condition

The first condition for the mutual recognition of the electronic identification means by other Member States is that electronic identification means has to be issued under an electronic identification scheme that is included in the list published by the European Commission pursuant to Article 9 of the eIDAS Regulation. In other words, it must be said that the electronic identification scheme has to be notified under the eIDAS Regulation.

The process of electronic identification scheme notification is carried out in several steps. In the first step, the Member State will provide at least 6 months prior to notification under Article 7 (g) of the eIDAS Regulation the description of the electronic identification scheme to other Member States and the European Commission (pre-notification). After that, a peer review of electronic identification schemes will take place, which can take up to 3 months.⁷ Such a review shall ensure that the electronic identification scheme complies with the interoperability framework and meets the requirements for assurance levels under the eIDAS Regulation.⁸ Member States can initiate the review through the Cooperation Network.⁹ The peer review will end with the issue of an official opinion which discusses whether the electronic identification scheme meets or does not meet the required standards. If the official opinion is positive, the notifying Member State will issue a formal notification to the European Commission. The European Commission is required to publish the notified electronic identification scheme in the Official Journal of the European Union within 2 months of notification. After notification, Member States have pursuant to Article 6 of the eIDAS Regulation 12 months to start recognizing electronic identification schemes. A clear overview of the time frame of the electronic identification scheme notification process is given in the following table.

Table 1: The time frame of the process of the electronic identification scheme notification

The time frame of the process of the electronic identification scheme notification	
1	Providing a description of an electronic identification scheme to other Member States Article 7 (g) of the eIDAS Regulation <i>At least 6 months before the notification</i>
2	Peer review <i>May take up to 3 months</i>
3	Notification of the national electronic identification scheme to the European Commission Article 9 of the eIDAS Regulation <i>Within 2 months of the notification shall be published in the Official Journal of the European Union</i>
4	Publication of an electronic identification scheme in the Official Journal of the European Union Article 9 (3) of the eIDAS Regulation <i>Mutual recognition shall commence within 12 months of publication</i>
5	The obligation to mutually recognize electronic identification schemes

Source: Own arrangement

The first Member State that provided a description of the electronic identification scheme was the Federal Republic of Germany (hereinafter referred to as the “Germany”) on 20 February 2017.¹¹ On 28 June 2017, the Cooperation Network issued an opinion that the documents describing the German electronic identification scheme (German Electronic Identity Card) demonstrate the fact that the German electronic identification scheme qualifies for notification under the eIDAS Regulation at an assurance level high. In the case of the official notification and publication of an electronic identification scheme in the Official Journal of the European Union, citizens of Germany will be able to authenticate into online services provided by other Member States.¹²

It is necessary to point out that Member States should not be obliged to notify their electronic identification schemes to the European Commission.¹³ The choice to notify the European Commission of all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States.¹⁴ In the context of the notification or non-notification the electronic identification scheme it should be noted that Member States will be obliged to recognize electronic identification means notified in accordance with the eIDAS Regulation from September 2018. In other words, if for example, the citizen of Germany wants to use the online service provided by the public authorities of the Slovak Republic and Germany has notified the electronic identification scheme in accordance with the eIDAS Regulation, the citizen of Germany has the right to authenticate for the use of such a service.¹⁵

3.2 The second condition

The second condition for the mutual recognition of the electronic identification means by another Member State is to ensure the assurance level of the electronic identification means (electronic

⁵ Details of the minimum technical specifications, standards and procedures setting out the assurance levels are regulated by Commission implementing regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of the eIDAS Regulation.

⁶ Article 6 of the eIDAS Regulation.

⁷ *Ibid.*, Article 12 (6) (a) in connection with Article 2 (b) of Commission implementing decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of the eIDAS Regulation.

⁸ For the interoperability framework that is created for the purpose of interoperability of national electronic identification schemes see Article 12 of the eIDAS Regulation.

⁹ Available at: <https://ec.europa.eu/cedigital/wiki/display/EIDCOOPNET/eIDAS+Cooperation+Net+work>.

¹⁰ More on the issue of the Cooperation Network and peer review in Commission implementing decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of the eIDAS Regulation.

¹¹ Available at: https://www.bsi.bund.de/EN/Topics/ElectrIDDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html.

¹² Italian Republic also officially pre-notified the national electronic identification scheme - SPID (Sistema Pubblico per la gestione dell'Identità Digitale). It is the first national electronic identification scheme to be notified under the eIDAS Regulation that is led by the private sector. Available at: <https://ec.europa.eu/digital-single-market/en/news/first-private-sector-eid-scheme-pre-notified-italy-under-eidas>. Republic of Croatia is preparing for process of notifying an electronic identification scheme called NIAS - National Identification and Authentication System in February 2018.

¹³ From the point of view of eGovernment evaluation, it is important for the Slovak Republic that the Slovak electronic identification scheme will be notified.

¹⁴ Preamble (13) of the eIDAS Regulation.

¹⁵ Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means.

identity card or other token of a person who wants to use an electronic service in another Member State) corresponding to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high.¹⁶

In other words, public sector body from the Member State A requires substantial or high assurance level for access to its online service. If the citizen of Member State B has the electronic identification means at the same or higher assurance level as required by the public sector body of the Member State A, the condition is fulfilled.

3.3 The third condition

The third condition for the mutual recognition of the electronic identification means is that the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.¹⁷

An electronic identification means which is issued under the electronic identification scheme included in the list published by the European Commission pursuant to Article 9 of the eIDAS Regulation and which corresponds to the assurance level low may be recognized by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies. In other words, it is up to Member States if they recognize the electronic identification means which corresponds to the assurance level low.

It is necessary to point out that access to online services and their final provision to the applicant is connected with the right to use such services under the conditions laid down in national law. In other words, even if a person can be electronically authenticated to access the online service of another Member State, he does not automatically have the right to use a particular online service, since such authorization may be subject to the condition of citizenship or permanent residence in specific country, and so on.¹⁸

4 Application issues

The fact that from 29 September 2018, the Slovak Republic will be obliged to recognize electronic identification means (notified according to the eIDAS Regulation) for the purposes of access of citizens of the European Union to Slovak public administration electronic services, gives a rise to many technical and mainly legal issues. Questions of a legal nature reveal if the legal system of the Slovak Republic reflects the changes that have occurred in the field of electronic identification and authentication and whether it creates a sufficient legal environment for potential foreign users of Slovak public administration electronic services.

4.1 Online service

The most important issues include the absence of a definition and absence of a defined range of online services. The eIDAS does not define the term online service but it mentions it in several places. It is clear from the provisions of the eIDAS Regulation that any service, whether public or private that is provided by using information and communication technologies (in particular the Internet, computing, etc.) can be considered as online service. Based on the above, a distinction can be made between public and private online services.¹⁹

From the provision of Article 6 (1) of the eIDAS Regulation indirectly implies that a public online service can be understood as a service provided online by public sector bodies.²⁰ The eIDAS Regulation does not define online service provider in detail but in general, it can be said that it is a natural person or a legal entity as well as an organizational component of the state. Online services providers may be considered (i) public sector entities or (ii) private sector entities.²¹ The crucial fact is that these entities require remote identification and authentication of the person by accessing their online service through an electronic identification means that is part of the electronic identification scheme notified under the eIDAS Regulation.

Furthermore, the term public service is also used in the eIDAS Regulation. Pursuant to the preamble (12) of the eIDAS Regulation “one of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services.” The eIDAS Regulation does not define the term public service in more detail.

From the perspective of Slovak legal order, it is necessary to point out that the definition of public online service is absent. Therefore, it is necessary to find the most suitable equivalent to the term public online service in Slovak legal order. I am of the opinion that under the conditions of the Slovak legal order, the term public administration electronic service may be considered the most appropriate equivalent of the term online service provided by public sector body. Even though the term public administration electronic service is broadly used, the real meaning is unclear. The term in question is mostly connected with the issue of the eGovernment which is regulated by Act No. 305/2013 Coll. on the Exercise of Public Authorities Competences in Electronic Form and on changes and amendments to certain acts (hereinafter referred to as the “e-Government Act”). The main aim of the e-Government Act is to embody official electronic communication as a primary form of communication between persons (individuals and legal entities) and public authorities as well as between public authorities themselves.²²

Provisions of e-Government Act apply only to cases when the decision issued is relating to rights, interests protected by law and obligations of natural persons or legal entities. Furthermore, the provisions of e-Government Act are limited to proceedings which result in issuing a decision as an individual legal act.²³ The e-Government act defines official electronic communication and other institutes necessary for exercise of public authority in electronic form, however the definition of the term public administration electronic services is absent.²⁴

²⁰ Pursuant to Article 3 (7) of the eIDAS Regulation public sector body means:

- (i) a state, regional or local authority,
- (ii) a body governed by public law or
- (iii) an association formed by one or several such authorities or one or several such bodies governed by public law, or
- (iv) a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate.

In the case of the term a body governed by public law the eIDAS Regulation refers to the term public institution stated in Article 2 (1) (4) of the Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.

²¹ Identification and authentication through the electronic identification means (e.g. an electronic identity card) is not limited only to online services provided by public sector bodies. There is an assumption that in the future private sector entities will also be able to accept the electronic identification means like electronic identity card or other means issued by the state to access their online services.

²² Official electronic communication is defined as electronic communication where the official electronic message which consists of an electronic application and official electronic documents, including attachments, is transmitted.

²³ The e-Government Act applies to public authorities. The term public authority (as institution) is broader than the term public administration authorities. More on terminology and structure of public administration authorities in: ANDRAŠKO, J., ŠURKALA, J.: *The concept of local self-government in the Slovak Republic. In Administrative law and process*, 2015, Vol. 12, Issue 2, p. 321-332. Available at: <http://aplaw.knu.ua/2015-2.pdf>.

²⁴ More on the issue of electronic services in: ANDRAŠKO, J.: *Theoretical aspects of public administration electronic services. In Bratislava law review*, 2017, Vol. 1, Issue 2, p. 119-128. See also: SOPÚCHOVÁ, S.: *Predpoklady fungovania e-governamentu v Slovenskej republike. In QUAERE 2015. Hradec Králové: Magnanimitas*, 2015, p. 659-668.

¹⁶ Article 6 (1) (b) of the eIDAS Regulation.

¹⁷ *Ibid*, Article 6 (1) (c).

¹⁸ E.g. public administration electronic service related to welfare services or in the case of the introduction of electronic elections in the National Council of the Slovak Republic or in the bodies of territorial self-government.

¹⁹ Preamble (2) of the eIDAS Regulation “this Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.”

The only legal act defining the term public administration electronic service is Act No. 275/2006 Coll. on Information Systems of Public Administration (hereinafter referred as the "ISPA Act"). In accordance with Section 2 (1) (s) of the ISPA Act are public administration electronic services defined as "electronic form of communication with liable parties²⁵ in the handling of submissions, notifications, access to information and their provision or public participation in the administration of public affairs".

It is necessary to point out that it is clear from the definition of the term public administration electronic services pursuant to the ISPA Act that the term in question does not apply only to decisions relating to rights, interests protected by law and obligations. The term in question defined in the ISPA Act includes submissions, notifications, access to information and their provision as well as public participation in the administration of public affairs. It can be said that in the case of the ISPA Act definition of the term public administration electronic services, there is a wide range of acts that can be done by persons in electronic communication with liable parties.

It is necessary to bear in our minds that not all public administration electronic services are relevant in the context of the eIDAS Regulation. Only those public administration electronic services are relevant where the identification and authentication of a person is required by use of an electronic identification means to access such a service. In the Slovak republic can be relevant at least those online services that we authenticate with an electronic identity card.²⁶

4.2 Slovak online service

In order citizens of other Member States could use online services provided by Slovak public sector bodies (hereinafter referred to as the "Slovak online services"), successful authentication through their national electronic identification means is required. The eIDAS Regulation does not explicitly specify to which Slovak online services can citizens of Member States authenticate themselves.

In my opinion, only those Slovak online services can be considered where identification and authentication are required and to which we can authenticate through the Slovak electronic identity card.

As mentioned above, successful authentication into Slovak online service by citizen of another Member State does not automatically authorize him to use of such a service. The access to online services and their final provision to the applicant is connected with the right to use such services under the conditions laid down in national law. In these cases, we talk about authorization. Successful identification and authentication is a prerequisite for authorization. Authorization is the permission to act in accordance with the privileges that are attached to that person.

In the light of aforementioned, it is necessary to select Slovak online services in two ways. Firstly, it is necessary to define Slovak online services where identification and authentication is required. Secondly, Slovak online services that can be really provided to citizens of other Member States have to be defined. As mentioned before, in many cases a legitimate condition (permanent residence, nationality, etc.) is established and such a condition prevents actual provide of such a service.²⁷

4.3 Assurance levels

Security in public online services is one of the key factors affecting the use of pertinent services. Security aspects do not represent only a technical dimension but also a legal one. According to the eIDAS Regulation, specific levels of assurance (low, substantial or high) shall be established for:

- a) electronic identification means,
- b) public online service,

Ad a)

There is a methodology for determining the assurance for the electronic identification means in the Slovak legal order, in particular Annex no. 6 of Regulation No. 55/2014 Coll. on Standards for Public Administration Information Systems (hereinafter referred as the "Annex 6").²⁸ Aforementioned legal framework is out of date in the Slovak Republic and in contrary to the eIDAS Regulation. The eIDAS does not contain provisions that would interfere with the national methodology for determination of the assurance levels. However, it would be appropriate to repeal the Annex No. 6 and replace it with a new methodology that would duplicate the methodology for determination of the assurance level under the eIDAS Regulation.

Ad b)

Under the third condition for mutual recognition of electronic identification means, the relevant public sector body uses in relation to access their online service assurance level substantial or high. This condition implies that the relevant public sector body and thus the Slovak online service provider is obliged to set a specific assurance level for access to the online service. In general, different assurance levels may be set for access to different Slovak online services. The eIDAS Regulation does not specify how the assurance level for a particular online service should be determined. The procedure for determination of the assurance level for access to the online service should be regulated at national level.

In that regard, it is necessary to find out which electronic identification means is used for purposes of identification and authentication to a specific Slovak online service. After that, the assurance level of electronic administration means will be set.

In practical terms, for Slovak online services where authentication can be made only by an electronic identity card, the assurance level will be set at a high level, as it can be assumed that the Slovak electronic identity card should have the highest assurance level according to the eIDAS Regulation.

Another situation can arise in cases where it is possible to authenticate to particular Slovak online service by another means (e.g. name and password). Here is a lower assurance level.

In the case if it is possible to authenticate to particular Slovak online service by an electronic identity card (assurance level high) and at the same time by another means (assurance level substantial) the final assurance level is set according to the lower level.

The eIDAS Regulation does not define specific entity which is liable for determination of the assurance level to particular online service. I believe that in the case of the Slovak Republic, the entities in question should be the providers of Slovak online services.

4.4 Sanctions

The legal order of the Slovak Republic will also have to deal with the legal liability for non-compliance with the eIDAS

²⁵ The list of liable parties is stated in Section 3 (3) of the ISPA Act. These parties are also known as administrators of information systems of public administration.

²⁶ The most used official authenticator in the Slovak Republic is electronic identity card. Such an authenticator is made up from identity card and electronic chip. More on the issue of electronic identity card in: ANDRAŠKO, J.: *Elektronický občiansky preukaz a iné spôsoby autentifikácie pri prístupe k elektronickým službám verejnej správy*. In QUAERE 2017. Hradec Králové: Magnanimitas, 2017, p. 235-244.

²⁷ The conditions for using a particular Slovak online service by citizens of other Member States must not be discriminatory. I advocate that we can restrict access to Slovak online services for the purpose of determining the condition of permanent residence, nationality, etc., if this is not contrary to European Union law.

²⁸ This methodology refers to the repealed Act No. 215/2002 Coll. on the Electronic Signature and to amend and supplement certain acts and to the STORK (*Secure identity across borders linked*) methodology, which refers to the repealed Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Regulation obligations. It is still unclear what sanctions can be imposed on Slovak online service providers for failing to allow the citizens of the European Union to authenticate and use a particular public service. The current legislation also does not reflect the situation where the provider of Slovak online service does not provide or provides an improper assurance level for specific public online services. I am of the opinion that it is necessary to adopt a generally binding legal regulation or to amend the existing related legislation that would regulate specific obligations and liability issues in relation to the determination of the assurance level under the eIDAS Regulation.

5 Conclusion

Adoption of the eIDAS Regulation is an important milestone in the lives of all European Union citizens. For the first time, a common legal framework has been created to enable cross-border authentication into online services provided by other Member States, whereby a citizen can use the domestic electronic identification means.

Mutual recognition of electronic identification means brings many challenges for Member States. Meeting these challenges can help to improve and increase in efficiency the delivery of eGovernment services so that citizens can identify and authenticate themselves simply, safely and with sufficient confidence.

The Slovak Republic over a long period creates the conditions for its citizens to be identified and authenticated for the use of eGovernment services but by adoption of the eIDAS Regulation it must ensure that citizens of other Member States who have notified electronic identification scheme under the eIDAS Regulation can authenticate to online services provided by Slovak public sector bodies.

Tasks that the Slovak Republic and other Member States must meet by 29 September 2018 concern in particular the creation of a node, the definition of online services to which citizens of other Member States can identify and authenticate and which they can actually use. It will be also necessary to establish assurance levels for online services provided by public sector bodies.

Meeting the abovementioned tasks will also result in many changes in the legal order. These changes will in particular affect the e-Government Act, which is the basic legal framework governing the identification and authentication of persons in cyberspace.

Literature:

1. ANDRAŠKO J.: *Electronic identification and authentication in the context of electronic public administration services*. In CER Comparative European research, 2016, Issue. 2, p. 75-78. ISBN 978-0-9935191-3-0. Available at: http://www.sciemcee.org/library/proceedings/cer/cer2016_proceedings02.pdf
2. ANDRAŠKO J., ŠURKALA J.: *The concept of local self-government in the Slovak Republic*. In Administrative law and process, 2015, Vol. 12, Issue 2, p. 321-332. ISSN 2227-796X. Available at: <http://aplaw.knu.ua/2015-2.pdf>
3. ANDRAŠKO, J.: *Theoretical aspects of public administration electronic services*. In Bratislava law review, 2017, Vol. 1, Issue 2, p. 119-128.
4. ANDRAŠKO, J.: *Elektronický občiansky preukaz a iné spôsoby autentifikácie pri prístupe k elektronickým službám verejnej správy*. In QUAERE 2017. Hradec Králové: Magnanimitas, 2017, p. 235-244. 978-80-87952-20-7.
5. SOPÚCHOVÁ, Soňa: *Predpoklady fungovania e-governmentu v Slovenskej republike*. In QUAERE 2015. Hradec Králové: Magnanimitas, 2015, p. 659-668. ISBN 978-80-87952-10-8.
6. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and

trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

7. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.

8. Commission implementing regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of the eIDAS Regulation.

9. Commission implementing decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic.

10. Act No. 275/2006 Coll. on Information Systems of Public Administration.

11. Act No. 305/2013 Coll. on the Exercise of Public Authorities Competences in Electronic Form and on changes and amendments to certain acts.

12. Regulation of Ministry of Finance of the Slovak Republic No. 55/2014 Coll. on standards for public administration information systems

13. <https://ec.europa.eu/cefdigital/wiki/display/EIDCOOPNET/eIDAS+Cooperation+Network>

14. https://www.bsi.bund.de/EN/Topics/ElectrIDDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html

15. <https://ec.europa.eu/digital-single-market/en/news/first-private-sector-eid-scheme-pre-notified-italy-under-eidas>

Primary Paper Section: A

Secondary Paper Section: AG