

LEGAL ASPECTS OF IMPLEMENTING DIGITAL SIGNATURES IN PAPERLESS BANKING



UDC 004.738.5:347.189(4-672EU:497.11)
336.71(497.11)
339.1:004

Sead Kadrić¹, Imran Rašljanin²

¹University of Graz, Graz, Austria

²State University of Novi Pazar, Novi Pazar, Republic of Serbia

ORCID iDs: Sead Kadrić
Imran Rašljanin

 <https://orcid.org/0000-0001-5731-9360>
 <https://orcid.org/0000-0003-1193-2746>

Abstract. *Integrating electronic signatures into paperless banking projects offers a transformative opportunity to streamline transactions and increase efficiency. However, this innovation is not devoid of legal challenges, especially within the framework of the eIDAS Regulation. This article examines the key legal hurdles encountered when implementing electronic signatures in paperless banking under the eIDAS Regulation. We examine the following topics: the legal validity of electronic signatures, the identification and authentication of signatories, and the establishment of secure electronic signature systems that comply with eIDAS requirements, as well as the liability and evidentiary considerations associated with electronic transactions. We highlight the need for financial institutions to put in place robust mechanisms to ensure compliance with eIDAS standards while navigating the complex legal landscape surrounding electronic signatures in paperless banking. By addressing these challenges, financial institutions can realize the full potential of electronic signatures to revolutionize the banking industry while maintaining legal integrity and regulatory compliance.*

Key words: *digital signatures, electronic signatures, paperless banking, Serbia, eIDAS Regulation, legal risks.*

1. INTRODUCTION

Regardless of whether it is a bank statement, reports, documents for opening a bank account or even signing a contract with a bank, paper has been an indispensable tool for banks over the last two centuries. Digitalization and paperless banking now make it possible to effectively reduce paper usage. What does "paperless" signify? It is not solely about imposing

Received March 27th 2024 / Accepted April 24th 2024

Corresponding author: Sead Kadrić, LL.M., MA student at University of Graz, Graz, Austria
e-mail: seadk67@gmail.com

a strict prohibition on paper but, rather, it involves considering whether printing or manual form filling at each stage of work is truly the most efficient approach. By prioritizing digital tools, banks allocate more time to serving their customers, enhance the quality of advice and data, and streamline error tracking. Additionally, banks promote resource conservation, setting a significant environmental example. While acknowledging that paper remains necessary in certain scenarios, we anticipate a huge reduction in excessive paper consumption in the future.

After 10 years since the adoption of eIDAS Regulation¹, banks are still trying to tackle the obstacles in order to fully realize one of their main goals when it comes to ESG projects (on environmental, social, and governance issues) and incorporating sustainable development into their businesses – paperless banking. Although the letter E in ESG (referring to environmental measures) may not seem to have a huge impact when it comes to measures imposed directly on banks and their organization, as they neither produce nor sell products which could be harmful for the environment (except the bank cards, which are made of plastic material and therefore non-recyclable), they still provide and sell services, which also entail the use of paper. It raised the key question about paper usage: To what extent is the use of paper necessary? To answer this question, banks started analyzing every single process that is performed by the organization and tried to remove the paper usage from the “equation”. Very soon they concluded that most of the processes involving paper could be digitalized, with only one important factor determining the possibility of paperless process – the risk of possible legal issues because of the document’s sole existence in digital form. The document by itself does not raise the question of validity, but the electronic signature and other forms of electronic identification (electronic seals, time stamps, etc.), which are on that document and which are usually mandatory, do. Nowadays, the term “digital signature” includes a wide spectrum of forms in which it can appear, and which have different legal validities. The forms of a digital signature can differ, ranging from a typed name on a document and a scanned handwritten signature to a digital signature made through public key cryptography, whereas even a click on the "I agree" button counts as an electronic signature. As long as there is a means to identify the signer, and it reflects one’s intention regarding the content of the electronic communication, all these signature forms meet the requirement akin to signatures on paper (Prokić, 2016:274). Therefore, in this article, we will focus on two situations, each of which may entail unique legal problems:

- 1) the situation where the document was physically hand-signed and then digitalized;
- 2) the situation where the document is digitally signed.

As for banking, it should be noted that this sector also uses all three types of electronic signatures prescribed by the eIDAS Regulation (2014), and that different types of electronic signatures are used for different bank documents. The goal of the "Paperless Banking" project is to enable legal transactions to be carried out and concluded with as little paper as possible, which would not be possible without a valid electronic signature that the bank or a client would sign via a specific device. There is also the question of choosing the type of electronic signature to make the legal transaction valid. This project is further complicated by the fact that the catalog of documents issued by the bank to both individuals and legal entities often exceeds over a thousand types. As the law is rapidly changing, it implies constant changes in the catalog of documents, whose number can fluctuate significantly during the year.

¹ Regulation (EU) 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: the eIDAS Regulation, 2014)

2. LEGAL FRAMEWORK FOR DIGITAL SIGNATURES IN PAPERLESS BANKING

Although the Directive 1999/93/EC² was in force for one and a half decade, the technological advancements expanded at such a rapid rate and to such an extent that the legislation simply could not keep up with such development. The advancement of technology in electronic commerce opened up a number of legal gaps which had to be precisely regulated. Soon, there was the need for a new and more precise regulation in the field of the electronic commerce and everything related to it (incl. electronic signatures). Thus, the eIDAS Regulation was passed in order to achieve certain goals more quickly.

As stated in the introductory part of the eIDAS Regulation, one of the main goals is to enable natural and legal persons to use national electronic identification mechanisms when using electronic services in any of the countries that make up the single market. The inherent characteristics of electronically stored data render it more susceptible to manipulation when compared to conventional data formats, thus necessitating detailed regulations on the preservation and validation of data integrity throughout its acquisition and exchange, ensuring that electronic evidence remains unaltered from its inception, storage, or transmission (Biasiotti, 2017: 3). In addition, the aim of the eIDAS Regulation is to create a single market for (electronic) trust services: qualified electronic certificates, seals, time stamps, and electronic document delivery. The ambition of this project is to ensure the legal security of using various trusted services that are both safe and easy to use, as this is a prerequisite for the adoption of these services by citizens as well as small and medium-sized enterprises. Only then would the world be able to overcome the lack of trust, in particular lack of legal certainty, that makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services. (Smedinghoff, Bro, 1999:728)

On the basis of the eIDAS Regulation (2014), Serbia passed a new law in 2017, the Act on Electronic Document, Electronic Identification and Trust Services in Electronic Business (hereinafter: the Electronic Document Act)³, which regulated electronic business and electronic signature. Thus, the Republic of Serbia took an important step in harmonizing Serbian law with EU law regarding electronic business. Compared to the countries of the European Union, Serbia started to regulate this matter relatively late but with this law Serbia clearly expressed the commitment to EU membership. The Electronic Document Act also distinguishes different types of electronic signature, whereby the terms and definitions of all electronic signatures are copied from the eIDAS Regulation.

The eIDAS Regulation defines three types of electronic signatures: simple, advanced and qualified electronic signature. All types of signatures are legally binding, but their evidentiary value varies. The simple electronic signature does not have to contain any identification information and is, therefore, hardly provable. Even if it is legally valid, it is not relevant to most business processes. As for advanced electronic signatures, the data recorded in a signature enable the signature to be assigned to the signatory. This form of signature is most frequently used in electronic commerce because it is easy to create, legally secure and provable. The qualified electronic signature requires identification before signing. This form takes more time and is, thus, typically used only for contracts where the law requires a written form. It means that the signature must be made on paper or via qualified electronic signature.

² Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

³ Act on Electronic Document, Electronic Identification and Trust Services in Electronic Business, *Official Gazette RS*, 94/2017 and 52/2021.

3. DOCUMENTS HAND-SIGNED AND THEN DIGITALIZED

The Electronic Document Act stipulates that an electronic document created by digitizing an original document whose form is not electronic is considered a copy of the original document (Article 10 § 4 of the ED Act). A document that has been digitized has the same evidentiary value as the original document if the following conditions are cumulatively met:

- 1) the digitization was carried out in one of the following ways, i.e. under supervision:
 - (1) a natural person or an authorized person of a natural person in the capacity of a registered entity or an authorized person of the legal entity whose document it is, or
 - (2) a person authorized to certify signatures, manuscripts and transcripts in accordance with the law governing the certification of signatures, manuscripts and transcripts, or
 - (3) persons who are authorized by special law to certify the digitized document.
- 2) the identity of the digitized document with the original one is confirmed by a qualified electronic seal or a qualified electronic signature of the person referred to in points (1)-(3) of this paragraph, or the person who was transferred the competences based on which the document was adopted (Article 11 § 1 of the ED Act).

On the basis of the aforesaid article, we see that the conditions for recognizing the equal evidentiary value of a digitized document can be very complex and that, in certain situations, it can create a huge problem for banks in the evidentiary procedure. Thus, in Serbia, in the period from 2019 to 2022, banks had a big problem when their clients started massively filing lawsuits against banks due to unjustified processing of loan costs. In that period, it is estimated that over 200,000 proceedings regarding these disputes were initiated before the court (N1 Info/Ilić-Krašić, 2022). The magnitude of this problem was influenced by a number of factors. First of all, the lawsuit for establishing nullity (which clients submitted in order to partially annul the provisions of the contract regulating the costs of loan processing) does not have a preclusion or limitation period in which it can be filed, so the clients also filed lawsuits regarding the contracts that the banks concluded with them since 2003 onwards.

This led to a situation where banks no longer had the original documentation in their possession, but submitted a copy of the scanned originals as evidence instead, which is under the Electronic Document Act regarded as a copy of the original document (this solution was also envisaged in earlier laws in Serbia). Therefore, their evidentiary value depended on whether the opposing party (i.e. the client) would dispute the authenticity of such a document by claiming that he neither signed that document nor that his signature was on that document. In such situations, the Civil Procedure Act (CPA)⁴ states that, if the document is submitted as a copy, the court will, at the request of the opposing party, order the applicant to submit the original document to the court, and the opposing party will be allowed to familiarize themselves with its contents. When it is necessary, the court will issue a decision on the deadline in which the document must be submitted, i.e. reviewed in the original or in a certified copy. No appeal is allowed against that decision (Article 100 § 3 and § 4 CPA).

Therefore, in any situation where the opposing party doubts the authenticity of the document, the court will ask the bank to submit the original document, which will inevitably result in a loss of the dispute for the bank whenever the document has been destroyed, either because the mandatory storage period has passed or because the original

⁴ Civil Procedure Act, *Official Gazette RS*, 72/2011, 49/2013, 74/2013, 55/2014, 87/2018, 18/2020 and 10/2023.

was digitized and then immediately destroyed (without being certified in terms of Article 11 Electronic Document Act). The obligation to attach the original is provided primarily for the eventual expert examination of the said document, given that the subject of the graphologist's expert examination can never be a copy of the document but only the original. This is also confirmed in the following legal reasoning of the Supreme Court judgment: "In the proceedings, the plaintiff, in order to prove his claim, proposed a graphological expert examination on that circumstance, but that expert examination was not carried out since it was established that the will was lost, and the court expert did not accept the graphological expertise to conduct the expert examination on the basis of a photocopy... As the original document of the will was not found, the prosecutor was unable to conduct an appropriate expert examination in a separate lawsuit and thus prove that the testator's signature on the will was forged."⁵

Given that the banks in these disputes often did not have original documentation precisely because the mandatory period for keeping such documentation had passed, they lost the dispute for the following reasons: "Since the authenticity of this document is disputed and the original or a certified photocopy of the said document has not been produced, the facts cannot be established on the basis of such a document, in which case it is the crucial fact, especially when the existence of such document and its veracity is essential, whereas the facts cannot be established based on other records".⁶ Due to such situations, banks should refrain from destroying the original documentation containing the signatures of any third parties, especially clients in situations where they digitize the document because such a move could cost them a legal case in the future if the digitization of that document was not preceded by an attestation. This is because the court can always accept the authenticity of the document issued by the bank, which includes only the signatures of employees or the seal of the bank, because such a document does not have signatures or any identification elements of third parties who would later contest the authenticity of such a document in a dispute.

Furthermore, the Civil Procedure Act of Serbia stipulates that, if the court doubts the authenticity of the document, it can request from the authority that issues such a document to declare it. (Article 238 § 4 CPA). It can be seen from this provision that the bank's statement alone will be sufficient for the court to determine the authenticity of the document, even in a situation where the original is no longer available, but there is only a digitized copy of the original, because in that situation there are no third party signatures which could be disputed, but only the signature an authorized person, i.e. an employee of the bank. Hence, it is certain that at some point in the near future, the issue of certification of the digitized paper documents will be a very important topic, bearing in mind that the current practice in Serbia regarding this procedure is almost non-existent, that the procedure itself is very complicated, and that in Serbia there is still no entity that is authorized by a special law to certify a digitized document based on the previously mentioned Article 11 § 1 (item 1, point 3) of the Electronic Document Act, and that the Register of Qualified Trust Service Providers does not show that such a service is performed by currently active registered providers (Ministry of Information and Telecommunication, 2024). Under the Act on the Registration Procedure with the Serbian Business Registers Agency (RP Act),⁷ there is only one case where the attorneys who represent

⁵ Judgement of Supreme Court of Cassation Rev 4898/2020 dated 18.02.2021

⁶ Judgement of Higher Court in Novi Pazar Gž 504/22 dated 28.07.2022

⁷ The Act on the of Registration Procedure with the Serbian Business Registers Agency, Official Gazette of RS, 99/2011, 83/2014, 31/2019 and 105/2021

a legal entity in the registration procedure with the Serbian Business Registers Agency can certify a copy of a digitized document, but only providing that they represent the legal entities in that registration procedure. Only in this case can an attorney certify the digitized document with his own electronic signature or qualified electronic stamp (Article 11a RP Act).

4. DOCUMENTS CREATED AND SIGNED DIGITALLY

When it comes to documents that were created in electronic form and signed digitally in one of the ways provided for electronic signature, it should be noted that Article 25 of the eIDAS Regulation stipulates that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. This article was directly inserted into the Serbian Electronic Document Act (Article 50). Further on, we will focus on the analysis of electronic signatures that are created in banking, considering that there are two most common ways of creating electronic signatures in this sector.

The first way is a digital signature pen pad which the client uses when signing the document. A signature pen pad is a small computer input device used to electronically record handwritten signatures. This means that it is an external hardware for signature digitization using a sensor (similar to a touchpad on a laptop), including input devices such as pens. This also includes monitors and/or monitor extensions with pen input, so-called pen displays (Signotec, 2024: 2). With this device, the client signs the document with his handwritten signature by pressing with a special pen on the surface specially designed for signature, which accurately records every movement of the pen as well as the pressure. It is important to keep in mind that such a signature does not physically leave a permanent trace anywhere but is automatically converted into an electronic form and saved as such on a document previously opened for signing, leaving a permanent trace only in digital form and in a specific document. What gives security to such a signature is that such a device usually registers the time when such a signature was made, but it does not necessarily have to be affixed to the document that was signed (it can be just one of the internal records that the device makes). What distinguishes this type of electronic signature is the identical procedure as the one in which the client signs his signature on paper.

The advantage of this type of signature is that its procedure is quite simple, and such a signature does not take more time when compared to a handwritten signature that the client would give on paper. Such devices are able to compare the signature with a previously saved copy (if the client has previously signed some documents), and to reject the signature or to request additional control by a bank employee, if there is no similarity with the saved copy. One of the most common situations where such a signature can be found is when withdrawing or transferring money from a savings account with a password (comprising one or two words) that the client must write via the signature pad, where the software can compare the signature with the previous one at the time of its entry, recognize the word through OCR technology, analyze the handwriting with the previous copy, and check if there is a high percentage of equivalence between the two signatures. Notably, with this type of savings account, money can also be withdrawn by a person who is not the account owner but who knows the password. In that case, entering the password via the signature pen pad records the handwriting of the person entering the password as well, which leaves the possibility of expert examination of that same password handwriting in court procedures in order to prove the identity of the person which entered that password.

Signatures given in this way are considered to be advanced electronic signatures because they enable a higher certainty in terms of the level of identification of the person giving the signature and provide additional security during the entire process of entering the signature into the document (the security of the interface and the internal records kept by the device). This method fulfills all the requirements for advanced electronic signature stipulated in Article 26 § 2 of the eIDAS Regulation (2014), which states that an advanced electronic signature is: “a) uniquely linked to the signatory; b) capable of identifying the signatory; c) it is created by using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and, d) it is linked to the data in such a way that any subsequent change in the data is detectable.”

The question arises as to the possibility of expert examination of such documents by a graphologist in case the client disputed such a signature. In our opinion, a graphologist should not refuse the expert examination of such a document, considering that such a document does not represent an ordinary copy of the original, because the document was created in electronic form, including the signature as well. Considering that in such a situation the signature was given manually on a device that automatically converted that signature into an electronic one, it could be compared with other signatures made by the client on paper because an expert may compare the specifics and equivalence of such an electronic signature and handwritten signature on paper (font size, handwriting, letter spacing, etc.). The expert examination of such a signature would not only be the task of a graphologist but also of an expert in the field of information technology because a graphologist can only examine certain types of document alteration (e.g. mechanographic activities) but cannot determine whether the signature was altered by mechanographic or computer activities, and thus falsified (e.g. by using a software) (Šarkić, Nikolić, 2014:131).

When it comes to the banking sector, there are several drawbacks of such a signature. The first one is reflected in the fact that such digital signature devices can only be used by the client inside the bank's branch office, bearing in mind that each of these devices is directly connected to the bank's computer and that each of them contains identification data which may be used later for determining the specific device on which a certain signature was given (which can also serve as evidence in court proceedings). Therefore, giving a signature remotely via this device is not possible. Another negative aspect of this type of signature is reflected in the fact that the client loses additional time due to coming to the branch office to sign the document. Thirdly, this signature is not considered a qualified electronic signature because the device through which the signature is given was not issued by an entity that provides a qualified trusted service, and the device itself is unable to request a prior fingerprint or facial authentication on the basis of which it authorizes the client to provide a signature, as is the case with a qualified electronic signature (although bank employees previously establish the person's identity on the spot with an official identification document). There is also a question regarding the fulfillment of written requirement when using this device, considering that the declaration text is not displayed on the signature pen pad but on the monitor of the corresponding computer; therefore, the signature is not placed below the declaration text. Our opinion is that this type of signature should meet the requirement of the written form because the intention of the signer in this situation is to agree and become legally bound by the text of the contract the moment when he gives the signature. We certainly believe that this type of signature will be among the qualified electronic signatures in the future, as soon as the banking sector finds an effective way to eliminate some of the previously mentioned shortcomings.

Another way clients can provide electronic signatures is through m-banking (the bank's mobile application) or through e-banking (the bank's internet portal). Due to the efficient implementation of electronic signatures in m-banking and e-banking, clients mainly sign and approve different types of documents and transactions. Thus, clients are able to sign a certain document at any time of the day and carry out the desired transaction without going to the bank (*Lečić-Cvetković, Omerbegovic-Bijelović, Zarić, Janičić, 2016:765*). It is important to point out that a qualified electronic signature can also be given in this way. Simply put, qualified electronic signature is just an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. The validity of a qualified electronic signature hinges on the verification process applied to it. It remains valid if, during signing, the accompanying certificate is a qualified one for electronic signatures, issued by an accredited trusted service provider and valid at the signing moment. Additionally, its validation data must match the data supplied to the relying party, along with a unique dataset representing the signatory as per the certificate. The integrity of the signed data remains intact provided that the creation tool for the qualified electronic signature is employed, and the prerequisites for advanced electronic signatures are fulfilled, thus preventing compromise (*Vukotić, 2021:153*). It should be noted that this does not imply entering a handwritten signature, as was the case with the signature pen pad; the document is signed with a single click on a button designated as "Sign" or "I agree". However, what makes it qualified is not the handwritten signature but the previous procedure of establishing the identity of the person giving the signature, as well as the protection of the platform where the entire procedure takes place. The possibility of providing such a signature proves that validity of the signature depends on the function it performs, not necessarily the form a signature takes (*Mason, 2016:208*). Therefore, for signatures given in m-banking or e-banking to have the legal effect of a qualified electronic signature, the m-banking application or the e-banking platform must implement some type of qualification tool for creating a remote electronic signature and possess a qualified certificate.

Given that banks are not authorized to perform such a qualified trust service themselves, when creating such an application or platform, it is necessary that a recognized provider of qualified trust services participate in the development of the m-banking application or e-banking platform (the list of providers is determined by the Ministry of Information and Telecommunications). In this way, banks are able to create a qualified electronic signature based on a smart card, USB key, or cloud. Bearing in mind that banks are guided by the efficiency of signature implementation, the most common way of implementing a qualified signature will be through the cloud. Thus, the entire electronic documentation is stored on the cloud server, without the risk of losing the "key" which is in the form of a smart card and a USB drive. Clients receive a document within the application or platform; they can read the content and, when signing, establish their identity by entering an additional code that they receive via SMS or email (in case of a two-factor authentication), facial authentication or a fingerprint, along with the app pin code or platform user password (*Đurić, 2021:90*).

Another way to establish identity is a face-to-face video call that clients have with a bank employee when opening an account. During the video call, they are asked to show their ID to the camera and make certain head movements or a certain hand gesture, in order for the bank employee to establish that it is a real-time transmission, and not a previously recorded video of that person. At the same time, one should be aware of the growing trend in the use of artificial intelligence which may be misused in such identification procedures (*Boljanović, 2019:31*). Due to the huge potential and risks underlying the use of AI, it is

quite reasonable to expect new laws or changes to the existing laws in the near future, which will additionally and more strictly regulate the application of electronic signatures and personal identification.

Due to the multitude of factors involved in the process of authenticating a person, it is certainly true that a qualified electronic signature makes this signature the most secure, and that is why this signature is equated with a handwritten signature when it comes to evidentiary value. The issue of concern in such processes is the validity of the feature that such a signature can never be given unintentionally. While a signature via the signature pen pad can certainly never be given unintentionally, for a qualified electronic signature (which is given with a single click) an argument could be made in front of court that the signature was mistakenly given through the application. The prior authentication process would not leave much room for such an argument because the process of authenticating the person giving the signature is set immediately before giving the signature itself, i.e. immediately before pressing the "Sign" or "I agree" button, and the person who does not intend to sign the document will certainly not enter the previously described authentication procedure.

Therefore, in the application, it is important to separate the process of familiarizing yourself with the content of the document and the process of giving a signature because, if both processes were preceded by only one authentication, the client could really argue that he/she signed such a document by an unintentional click while reading the content of that document, and thus try to prove that there was a lack of will. Namely, under the Civil Obligations Act⁸, the will shall be declared freely and seriously (Art. 28 § 2), and the will is considered declared and the contract is concluded at the moment when it is signed by all contracting parties (i.e. by the last party) assuming contractual obligations (Article 72 § 1). Since at that moment the internal and external (declared) will of the client did not match, it would mean that there was a deficiency of will; thus, one could argue in front of court that such a contract should be annulled for that reason (Mijačić-Cvetanović, 1982:180-181). It is also important to point out that this signature cannot be the subject matter of expert examination by a graphologist because it is not a handwritten signature that was created in electronic form but a combination of letters and numbers that the certificate automatically generates together with the name and surname in form of a plain text. Therefore, such a signature could only be examined by an expert in the field of information technology (Oparnica, 2016:143). It could be argued that proving the authenticity of a digital item involves examining claims and building trust. It is not about proving that an 'original' exists, especially with dynamic things like databases but about presenting enough evidence to convince someone that the retrieved item is a faithful representation of what is claimed to be the original, or a reliable version of what the creator used (Mason, Seng, 2017:230).

5. DETERMINING THE NECESSARY TYPE OF ELECTRONIC SIGNATURE

When talking about business within the banking sector, it is important to point out that there is no *numerus clausus* of documents that require a specific signature, but banks most often use the principle of written form in evaluating the use of signature types. This is one of the leading criteria used by the bank because the legislator often uses the written form as one of the essential elements of the contract that needs to be secured for the benefit of

⁸ The Civil obligations Act (Act on Contracts and Torts), *Official Gazette SFR Yugoslavia*, 29/1978, 39/1985, 45/1989, 57/1989, 31/1993.

both the contract (contracting parties) and third parties; such a document has a strong evidentiary force before the authorities (*ad solemnitatem* document). Thus, whenever the law prescribes that a certain type of documents or contracts should either be hand-signed or in a written form, it is safe to assume that qualified electronic signature is the required form since it is the only one that has the equivalent legal effect as a handwritten signature.

Once it is confirmed that there is no legal requirement for such a contract or legal transaction to be in written form, only then can the bank use any form of electronic signature that may be sufficient from a legal point of view. When choosing an electronic signature and communication channel, it is necessary to prioritize the verifiability of the content and ensure the agreement of the contracting parties, and to base the choice on this factor. Simply put, while electronic signatures do offer the flexibility, it is vital to consider the formal requirements, ensure the integrity of the content, and evaluate the associated legal risks when choosing an appropriate signature method (Höller, 2021:1089).

The complexity of the document issuance process should be another factor in determining the right type of signature. The more complex the process is, the better it is to use a higher form of electronic signature. For example, some documents require the four-eyes principle in order to be issued. The four-eyes principle means that a certain decision, transaction (etc.) must be approved by at least two people working in the bank. From the external point of view, even the simple electronic signatures would make no legal risk for the bank, as long as it reaches the customer through a trusted and secure communication pathway (e.g. through the bank app); from the internal point of view, in order to evade a potential risk of one employee abusing the process and typing in the name of the second person without his/her knowledge, each employee should put his/her qualified electronic signature on the document so that it cannot be forged by the other person.

As for other documents which entail a simple procedure when it comes to issuing them, the simple electronic signature should be sufficient since the bank document usually lists the responsible employee on the letterhead. In addition, the program usually automatically generates the user data of the employee in the footer of the document which was created or printed by the employee.

6. CONCLUSION

According to the Electronic Document Act, the integration of electronic signatures, electronic identification and trusted services in electronic business holds a promise of the significant expansion of paperless banking in Serbia. With the increasing adoption of mobile banking (m-banking) and electronic banking (e-banking) among bank customers for their transactions and business affairs, the legal framework surrounding electronic signatures is becoming increasingly important. Based on the report of the National Bank of Serbia (hereinafter: the NBS), in the period from 2014 to 2018 alone, the number of e-banking users increased from 1,153,611 to 2,465,904, while the number of m-banking users increased from 179,724 to 1,426,825. This also indicates that paperless banking was still in the initial stage of development at that time, especially the banking apps (Nikolić, Nikolić, 2019:213-215). The latest NBS report from 2024 records that, at the end of 2023, the number of e-banking users was 4,093,621, while the number for m-banking users was 4,044,375 (National Bank of Serbia, 2024). Based on this report, in 2024, the number of m-banking users is expected to exceed the number of e-banking users for the first time due to a higher growth rate of m-

banking. This indicates that banks should invest as much as possible in the development of mobile banking, and electronic signatures through these mobile applications. Despite the progressive legal framework that ensures the validity and legal equivalence of electronic signatures with traditional handwritten signatures, there are still challenges in their practical application. We can certainly conclude that there is still a certain degree of unfamiliarity and reluctance among judges and state authorities to fully accept electronic signatures, sometimes preferring traditional documentation in printed form. Efforts to increase awareness and understanding of electronic signature laws among stakeholders, especially in the banking sector, are essential to foster trust and acceptance of electronic signatures. In addition, simplifying procedures and expanding the availability of qualified electronic signature providers can facilitate the wider use of electronic signatures in paperless banking transactions. As paperless banking continues to expand in Serbia, joint efforts between government authorities, financial institutions, legal experts, and the business community are of utmost importance to navigate through the challenges and unlock the full potential of electronic signatures in modernizing and facilitating banking transactions in the digital era.

REFERENCES

- Biasiotti, M. A. (2017). Proposed Electronic Evidence Exchange across the European Union. *Digital Evidence and Electronic Signature Law Review*, 14, 1-12.
- Boljanović, V. (2019). Elektronski potpis u Srbiji i harmonizacija sa pravom Evropske unije: mogućnosti i izazovi (Electronic Signature in Serbia and Harmonization with EU Law: Possibilities and Challenges), Master Thesis, University of Belgrade.
- Đurić, D. (2021). Elektronski potpis i zašto ga (ne) primjenjujemo (Electronic Signature and why do we (do not) use it), *Godišnjak Pravnog fakulteta u Banjaluci*, 43(43), 83-99.
- Höller, A. (2021). Checkliste: Schriftlichkeit und Nutzung elektronischer Signaturen (Checklist: Writing and Use of Electronic Signature). *Ecolex*, 702, 1086-1089.
- Knežević, M., Šapić, S. (2018). Legal regulation and usage of electronic trade in Republic of Serbia. *Ekonomika (Niš, Serbia)*, 64(3), 1-22.
- Lečić-Cvetković, D., Omerbegović-Bijelović, J., Zarić, S., Janičić, R. (2016). E-banking application in business companies – A case study of Serbia. *Information Development*, 32(4), 762-776.
- Mason, S. (2016). *Electronic Signatures in Law*. University of London Press.
- Mason, S., Seng, D. (Eds.). (2017). *Electronic Evidence* (4th ed.). University of London Press.
- Mijačić-Cvetanović, M. (1982). O Manama volje prema Zakonu o obligacionim odnosima (On the deficiencies of will under the Civil Obligations Act), *Zbornik radova Pravnog fakulteta u Nišu*. 22/1982, 179-195.
- Nikolić, A., Nikolić, D. (2019). Digital Banking Transformation Development and Use of Electronic Banking in Serbia, Economic and Social Development. *International Scientific Conference on Economic and Social Development*, 41, 210-216.
- Oparnica, G. (2016). Digital Evidence and Digital Forensic Education, *Digital Evidence and Electronic Signature Law Review*, 13, 143-147.
- Prokić, D. (2016). The Adoption of the United Nations Convention on the Use of Electronic Communications in International Contracts in Serbia - a way to facilitate cross-border trade, *Anali Pravnog Fakulteta u Beogradu*, 64(3), 266-286.
- Šarkić, N., Nikolić, M. (2014). Veštačenje: građansko-pravni aspekt (Expert Examination: from the aspect of Civil Law). *Glosarijum*.
- Smedinghoff, T.J., Bro, R.H. (1999). Moving with change: electronic signature legislation as vehicle for advancing e-commerce, *John Marshall Journal of Computer and Information Law*, 17(3), 723-768.
- Vukotić, J. (2021). Uredba (EU) 910/2014 o elektronskoj identifikaciji i uslugama od poverenja za elektronske transakcije. (Directive (EU) 910/2014 on electronic identification and trust services for electronic transactions), *Evropsko Zakonodavstvo*, 20 (75), 145-156.

Legal Acts

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- 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.
- Act on Contracts and Torts (Zakon o obligacionim odnosima), *Official Gazette SFR Yugoslavia*, 29/1978, 39/1985, 45/1989, 57/1989, 31/1993.
- Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju (Act on Electronic Document, Electronic Identification and Trust Services in Electronic Business), *Službeni glasnik RS*, 94/2017 i 52/2021.
- Zakon o parničnom postupku (Civil Procedure Act), *Službeni glasnik RS*, 72/2011, 49/2013, 74/2013, 55/2014, 87/2018, 18/2020 i 10/2023.
- Zakon o postupku registracije u Agenciji za privredne registre (Act on the Procedure of Registration with the Serbian Business Registers Agency, *Službeni glasnik RS*, 99/2011, 83/2014, 31/2019 and 105/2021.

Judicial Practice

- Presuda Višeg suda u Novom Pazaru (Judgment of Higher Court in Novi Pazar) Gž 504/22 dated 28 July 2022.
- Presuda Vrhovnog kasacionog suda (Judgment of Supreme Court of Cassation RS) Rev 4898/2020 dated 18 February 2021.

Online Sources

- Ministarstvo Informisanja i telekomunikacija/Ministry of Information and Telecommunication (2024). Registar pružalaca kvalifikovanih usluga od poverenja (Register of Qualified Trust Service Providers), Retrieved 20 March 2024, from <https://mit.gov.rs/tekst/sr/583/registar-pruzalaca-kvalifikovanih-usluga-od-poverenja.php>
- Narodna banka Srbije/National Bank of Serbia (2024). Broj korisnika po vrstama određenih platnih usluga (Report on the number of users by type of payment service), Retrieved 20 March 2024 from <https://www.nbs.rs/sr/ciljevi-i-funkcije/platni-sistem/statistika/#>
- N1 Info/Ilić-Krasić, D. (2022). Udruženje banaka: Pred Vrhovnim sudom nekoliko hiljada postupaka revizije, (Association of Banks: Several thousand audit proceedings before the Supreme Court), N1 Info, Retrieved 15 March 2024, <https://n1info.rs/biznis/udruzenje-banaka-pred-vrhovnim-sudom-nekoliko-hiljada-postupaka-revizije/>
- Signotec (2024). End-User Licence Agreement for Signotec Software, <https://en.signotec.com/portal/dokumenteplus-900000292-10002.html>.

PRAVNI ASPEKTI IMPLEMENTACIJE DIGITALNIH POTPISA U BESPAPIRNOM BANKARSTVU

Integracija elektronskih potpisa u bankarske projekte bez papira nudi transformativnu priliku za pojednostavljenje transakcija i povećanje efikasnosti. Međutim, ova inovacija nije lišena pravnih izazova, posebno u okviru eIDAS Uredbe. Ovaj članak ispituje ključne pravne prepreke sa kojima se banke susreću pri implementaciji elektronskih potpisa u bespapirom bankarstvu u skladu sa eIDAS Uredbe, gde ćemo ispitati sledeće teme kao što su pravna valjanost elektronskih potpisa, identifikacija i autentifikacija potpisnika i uspostavljanje bezbednih sistema elektronskih potpisa, koji su u skladu sa zahtevima eIDAS Uredbe, kao i sa odgovornošću i razmatranjima u vezi sa dokazima u vezi sa elektronskim transakcijama. Takođe naglašava potrebu da finansijske institucije uspostave snažne mehanizme kako bi osigurale usklađenost sa standardima eIDAS Uredbe dok se kreću kroz složeni pravni pejzaž koji okružuje elektronske potpise u bankarstvu bez papira. Baveći se ovim izazovima, finansijske institucije mogu da ostvare puni potencijal elektronskih potpisa da revolucionišu bankarsku industriju uz održavanje pravnog integriteta i usklađenosti sa propisima.

Ključne reči: *digitalni potpisi, elektronski potpisi, bespapirom bankarstvo, eIDAS regulativa, Srbija, pravni rizici.*