World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-50, September-2025
ISSN: 2749-3601

DIGITAL IDENTIFICATION AND ELECTRONIC SIGNATURE: LEGAL, TECHNICAL AND SOCIAL ASPECTS

Alfiya Kazi - Regulatory Affairs Manager and legal expert. Kazakhstan

Article history:

Received: 6th July 2025
Accepted: 4th August 2025

Abstract:

The article is devoted to the analysis of the institute of digital identification and electronic signature as key elements of the trust infrastructure in the context of digitalization of society. The theoretical foundations and technological approaches to establishing identity in the electronic environment are considered, legal regulation in the Russian Federation, the European Union and a number of foreign countries is analyzed. Particular attention is paid to the types of electronic signature, their legal status and cryptographic foundations of functioning. The areas of application of digital identification and electronic signature in public administration, the financial sector and business are studied. The main problems and risks associated with ensuring cybersecurity, protecting personal data and biometric information, as well as overcoming the digital divide are identified. The prospects for the development of the institute are determined taking into account the introduction of blockchain technologies, artificial intelligence and harmonization of international regulation. It is concluded that further improvement of digital identification and electronic signature requires an integrated approach, including the development of a regulatory framework, increasing the level of security and strengthening public trust.

Scientific novelty

The scientific novelty of the study lies in the comprehensive consideration of digital identification and electronic signature not only as legal and technical categories, but also as a social phenomenon that forms the infrastructure of trust in a digital society. The work substantiates the need to analyze these institutions in the unity of legal norms, technological solutions and ethical restrictions, which allows us to identify their systemic nature. What is new is the emphasis on the conjugation of digital identification with biometric technologies, artificial intelligence and blockchain systems, which allows us to predict the further transformation of electronic interaction. An additional element of novelty is the identification of the relationship between the level of digital inequality and the effectiveness of the implementation of identification mechanisms, which opens up prospects for further research in the field of socio-technical risks of the digital economy.

Purpose of the study

The aim of the study is a comprehensive analysis of digital identification and electronic signature as key tools for ensuring trust in the digital environment, identifying the features of their legal regulation, technological implementation and social significance, as well as determining the prospects for their further development in the context of the digital economy and the transformation of public relations.

Keywords: digital identification, electronic signature, trust infrastructure, electronic legal regulation, biometric technologies, cybersecurity, digital economy.

INTRODUCTION

The transition of society to digital technologies has necessitated the search for new ways to confirm identity and ensure the legal validity of documents in the electronic environment. With the development of telecommunications networks and the advent of electronic document management, traditional identification methods based on the presentation of paper IDs or a handwritten signature no longer meet the requirements of the times. There is a need for tools that can guarantee the reliability of information and the trust of participants in interactions in the absence of physical contact.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-50, September-2025
ISSN: 2749-3601

Historically, the first attempts to create electronic analogues of a signature date back to the 1970s and 1980s, when asymmetric encryption methods were developed within the framework of cryptography, which made it possible to implement the principle of confirming the authenticity of data using a pair of keys. One of the significant stages was the emergence of the RSA algorithm in 1977, which laid the foundation for modern electronic signature systems. In the 1990s, the electronic signature received legislative recognition: in 1996, the Uniform Electronic Transactions Act was adopted in the United States, which secured the legal force of digital signatures, and in 1999, a similar act was adopted in the European Union.

In Russia, the development of the electronic signature institute began in the late 1990s and was associated with the need to switch to electronic document management in government agencies and the financial sector. The first regulations were fragmentary and regulated only individual areas of application of digital technologies. A breakthrough moment was the adoption of the Federal Law "On Electronic Signature" in 2011, which introduced a systemic classification of signature types and laid the foundations for the legal infrastructure of trust.

In parallel, digital identification systems have developed. In the early stages, they were based on passwords and logins, but were gradually supplemented by biometric technologies and multi-factor authentication methods. Estonia, Singapore and a number of other countries have demonstrated successful models for building national digital identification systems, which have become benchmark examples for the international community. In the European Union, the creation of a single digital trust space was ensured by the adoption of the eIDAS regulation in 2014.

Today, digital identification and electronic signature are an integral part of the infrastructure of the digital state, financial systems and business. Their significance goes beyond the technical function of identity verification and acquires the character of a social institution that ensures trust and legitimacy of electronic interaction.

The purpose of this study is a comprehensive analysis of digital identification and electronic signature, consideration of their historical development, legal and technological aspects, as well as identification of prospects for further development in the context of digitalization of the economy and public relations.

THEORETICAL FOUNDATIONS OF DIGITAL IDENTIFICATION IN THE CONTEXT OF DIGITALIZATION OF SOCIETY

The digitalization of society and the accelerated introduction of electronic services have set the state, business and citizens the task of creating new instruments of trust on the network. The mass distribution of electronic document management, remote banking, online services and other forms of communication is impossible without a clear system of identity verification and legal consolidation of actions taken. That is why digital identification and electronic signature are gradually becoming fundamental institutions of the digital economy, ensuring the security of interaction and the legitimacy of documents created in electronic form.

There is also the concept of a "digital signature" - this is information in electronic form that is linked to other electronic information and is used to identify the person using this information. [1]

Digital identification is the process of establishing and confirming identity in a virtual environment using special technical and organizational mechanisms. Unlike traditional identification, which is carried out on the basis of paper documents, digital identification allows remote confirmation of the identity of a citizen or organization. This can be done using the user's knowledge in the form of a password or code, items at his disposal, such as a mobile device, as well as body characteristics, such as biometric parameters. Over time, there is a tendency to move from single-factor authentication methods to multi-factor systems that can combine several approaches to increase reliability.

Legal regulation in this area is developing as states realize the critical role of trust infrastructure in electronic interaction. In the Russian Federation, the key regulatory document is the law on electronic signature, adopted in 2011, which established three types of electronic signature: simple, enhanced unqualified and enhanced qualified. Of particular importance is the Unified Identification and Authentication System, which serves as a kind of framework for the entire system of providing public services in digital form. Within this system, citizens gain access to the portal of public services and a variety of services provided by both government agencies and businesses.

In the European Union, the eIDAS regulation, adopted in 2014, serves as the foundation for legal regulation. It established uniform requirements for electronic signatures and trust services, thereby ensuring the mutual recognition of electronic identifiers in all countries of the union. This made it possible to create a harmonized space of digital trust, which is especially important for the functioning of the single market. International experience demonstrates many

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-50, September-2025
ISSN: 2749-3601

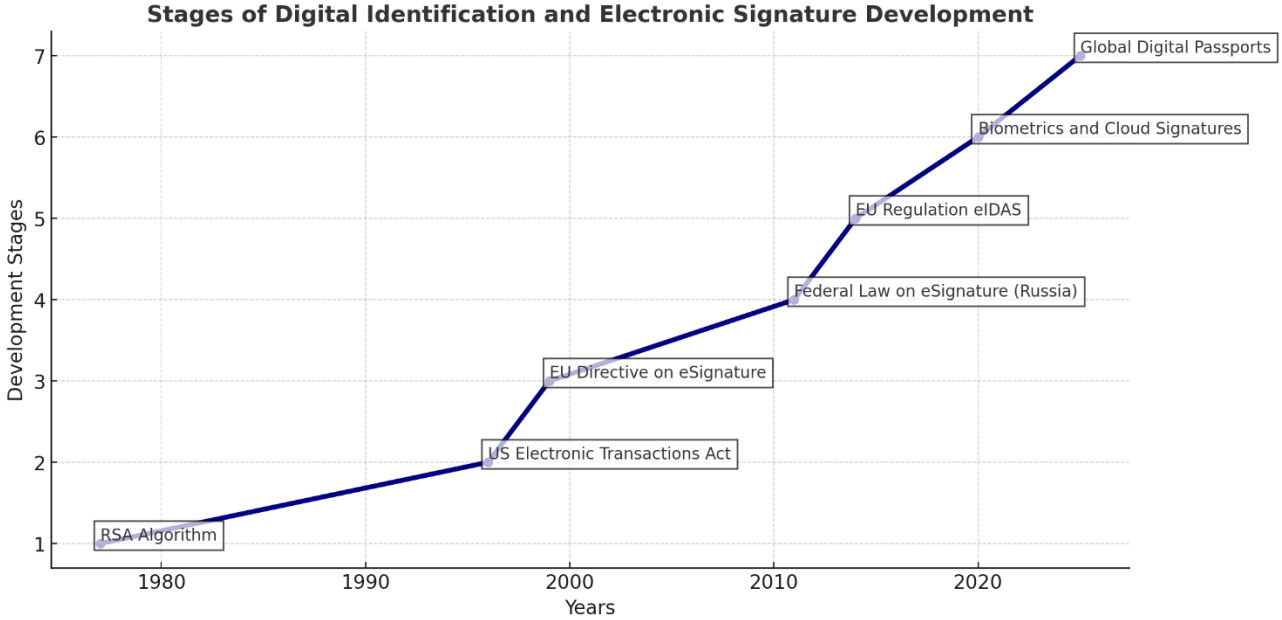
interesting solutions. For example, Estonia has become a pioneer in the field of digital identification, having created a system based on a national card and a mobile signature. Singapore is developing the SingPass platform, which allows citizens to access government and commercial services through a single digital identifier.

The electronic signature, in turn, performs key functions to ensure the legal force of electronic documents. It confirms the authenticity of the subject who signed the document, guarantees its immutability and provides the possibility of proof in court. From a technological point of view, the electronic signature is based on cryptographic algorithms of asymmetric encryption, which use a pair of public and private keys, as well as on the use of hash functions. The organizational basis for the functioning of the electronic signature is the public key infrastructure, including certification centers and certificate registries. In recent years, cloud solutions have become widespread, allowing users to sign documents from a mobile device without the need to use tokens and specialized tools.

However, the electronic digital signature itself needs to be improved. Since it is necessary to add evidence of authenticity, including various data about the certificate, such as a stamp. [2]

PRACTICAL APPLICATION OF DIGITAL IDENTIFICATION AND ELECTRONIC SIGNATURE

The practice of using digital identification and electronic signatures is diverse. In the sphere of public administration, they are used to provide electronic services, maintain government document flow, and implement remote voting projects. Financial institutions are implementing remote identification systems to open accounts, issue loans, and make payments. In Russia, a single biometric system is in operation for this purpose, allowing citizens to be identified by face and voice. In business, electronic signatures are used when concluding contracts, in accounting and tax reporting, and in electronic trading systems. International projects are aimed at creating cross-border digital identification tools, an example of which is the initiative to form a European digital wallet, which will provide citizens with access to services in different countries of the union.



The graph shows the key stages in the development of digital identification and electronic signature in global and Russian practice. The starting point is 1977, when the RSA algorithm was created, which marked the beginning of the practical application of cryptographic methods for protecting information and forming digital signatures. The next significant stage is associated with the mid-1990s, when the Electronic Transactions Act (1996) was adopted in the United States, which secured the legal force of digital signatures, and in 1999 the first directive regulating the use of electronic signatures was approved in the European Union.

For Russia, a fundamentally important moment was the adoption in 2011 of the Federal Law "On Electronic Signature", which defined the types of signatures and secured their legal status. In 2014, the EU adopted the eIDAS regulation, which ensured uniform rules for digital identification and trust services throughout the union. By 2020, the development of technologies led to the widespread implementation of biometric solutions and cloud electronic signatures, which significantly expanded the scope of application of digital services.

A promising direction for the near future, indicated in the graph, is the formation of global digital passports,

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-50, September-2025
ISSN: 2749-3601

which should ensure cross-border interaction and mutual recognition of electronic identifiers. Thus, the graph reflects the evolution from basic cryptographic developments to the formation of a comprehensive trust infrastructure covering national and international levels.

Despite the obvious advantages, digital identification and electronic signature are associated with serious problems and risks.

Table 1. Problems and risks of digital identification and electronic signature and ways to solve them

Problem	Content	Possible solutions
Cyber threats	Phishing, account hacking, certificate forgery, key theft	Strengthening cryptographic algorithms, multi-factor authentication, anomaly monitoring
Leakage of personal and biometric data	Illegal access to databases, insufficient information protection	Development of legal norms on data protection, use of encryption technologies, storage of data in distributed systems
Legal conflicts	Differences in legislation in different countries, lack of uniform standards	Harmonization of international standards, conclusion of interstate agreements, development of ISO standards
Digital Divide	Limited access to the Internet and modern devices among certain groups of the population	Digital inclusion programs, subsidized access to technology, digital skills training
User distrust	Security and privacy concerns	Increasing transparency of systems, informing citizens, independent audit of trusted services

One of the most significant is the threat of cyberattacks, including phishing, account hacking and certificate forgery. Leaks of personal data and biometric information pose significant risks, as they can undermine public trust in the system. Legal issues are related to differences in regulation between countries and the difficulties of mutual recognition of electronic signatures. One cannot ignore the social aspect, which is expressed in digital inequality: certain groups of the population still do not have stable access to the Internet and modern devices, which excludes them from digital interaction.

The prospects for the development of digital identification and electronic signatures are closely linked to the introduction of innovative technologies. Blockchain opens up the possibility of decentralized data storage and protection against counterfeiting. Artificial intelligence is actively being introduced into biometric identification systems and allows for the detection of suspicious actions in real time. The Internet of Things requires the development of authentication mechanisms for a growing number of devices interacting in a single network. Finally, the idea of global digital passports is on the horizon, which will simplify cross-border interaction and become a tool for global mobility.

The operation of a digital signature assumes that the private key is known only to its owner. If an outsider gains access to it, it becomes possible to create fake signatures and pass them off as signatures of the real owner. [3]

The validity period of the certificate is limited for information security purposes. It is usually issued for one year, after which it is subject to renewal. In the event of a threat of compromise of the private key (for example, if the key information carrier is lost or left unattended), if the password is lost or the owner's identification data is changed, the certificate is subject to revocation and replacement with a new one. [4]

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-50, September-2025
ISSN: 2749-3601

In conclusion, it should be emphasized that digital identification and electronic signature have already become the cornerstones of the trust infrastructure of modern society. They ensure security, legal significance and convenience of electronic interaction, which allows citizens and organizations to fully participate in the digital economy. At the same time, the future of these institutions depends on a harmonious combination of legal regulation, technological innovations and public trust. Development should be accompanied by an increase in the level of cybersecurity, ensuring the availability of services for all segments of the population and strengthening international cooperation. Only if these conditions are met will digital identification and electronic signature be able to realize their full potential and become the basis of the global digital trust infrastructure.

Regular passports are static documents that provide the same set of information about the owner in any situation. In contrast, an attribute-based electronic ID (eID) is personalized. The owner of such an eID has access to different categories and can disclose only the data that is necessary in a specific context. [5]

Today, public key cryptosystems are in the greatest demand, since their algorithms are built on the basis of the mathematical apparatus of elliptic curves. [6]

The list of references includes regulatory acts and scientific publications. Among the most significant are the federal law on electronic signature, the European Union eIDAS regulation, the international standard ISO 29115, as well as scientific works by Russian and foreign researchers devoted to the problems of legal regulation and technical implementation of electronic signatures. Particular attention in the scientific literature is paid to the experience of Estonia, which has shown that with an integrated approach it is possible to create a working model of a digital state. Researchers also emphasize the importance of taking into account ethical aspects and protecting human rights when using biometric technologies, without which it is impossible to ensure public confidence in digital tools.

CONCLUSION

The conducted research showed that digital identification and electronic signature are key elements of modern digital infrastructure, ensuring trust in the conditions of global digitalization. Their historical formation is closely connected with the development of cryptography and the spread of electronic document management, and legal consolidation became a response to the needs of the state, business and society in new forms of identity verification and legitimization of electronic documents.

It should be emphasized that modern encryption and verification methods, while highly reliable in encoding information, are not able to fully protect the user from the actions of unscrupulous individuals. However, this drawback does not diminish the significant advantages of using an electronic signature in the process of implementing electronic document management in various fields of activity. An electronic signature remains an effective and relevant instrument for certifying documents. [7]

Modern approaches to digital identification are based on the integration of multifactor authentication methods, including the use of biometric characteristics. The electronic signature, in turn, has evolved from the simplest means of recording electronic actions to complex cryptographic technologies recognized in national and international legal systems. The Russian legal framework in this area is actively developing, which allows for the expansion of the use of electronic services and strengthening trust in government and commercial structures. European and international experience demonstrates the need for unification and harmonization of rules, which is an important condition for the creation of a single digital space.

Despite significant achievements, this area faces a number of challenges. Among them are cyber threats related to the possibility of compromising personal data and biometric information, legal conflicts in cross-border interaction, as well as digital inequality, which prevents equal access of the population to modern services. The solution to these issues requires a comprehensive approach, including improving legislation, introducing reliable technological solutions and developing mechanisms to protect user rights.

Prospects for further development of digital identification and electronic signature are associated with the introduction of innovative technologies such as blockchain, artificial intelligence and the Internet of Things. In combination with strengthening international cooperation and developing uniform standards, this will create a global system of digital trust that ensures the security and sustainability of interaction in the electronic space.

It should be emphasized that, despite the key importance of the electronic digital signature for the digital business ecosystem, its implementation in all sectors of production and services will occur gradually. This is explained not only by the different degrees of technological readiness of economic entities to switch to new solutions, but also by the different levels of training of end users of information resources. [8]

Artificial intelligence in legal practice does not per se belong to legal technologies, being a digital information

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-50, September-2025
ISSN: 2749-3601

technology. However, its application by legal entities to achieve a specific legal result can be considered as the use of legal technology. [9]

Thus, digital identification and electronic signature are not only a technological and legal tool, but also an important social institution that forms the basis of the digital economy and the electronic state. Their development determines the direction of the transformation of social relations in the 21st century and requires constant attention from both legislators and specialists in the field of information technology, as well as from the whole society. [10]

REFERENCES

1. Annin Anatoly Gennadievich, Novikov Sergey Stepanovich ELECTRONIC SIGNATURE: CONCEPT AND PRACTICE OF APPLICATION // Agrarian and land law. 2020. No. 8 (188). URL: https://cyberleninka.ru/article/n/elektronnaya-podpis-ponyatie-i-praktika-primeneniya
2. Kurbatov A. D. PROBLEMS OF IDENTIFICATION OF ELECTRONIC DIGITAL SIGNATURE // Forum of young scientists. 2017. No. 5 (9). URL: https://cyberleninka.ru/article/n/problemy-identifikatsii-elektronnoy-tsifrovoy-podpisi
3. Shandrovich A.V., Demkin D.A. ELECTRONIC DIGITAL SIGNATURE IN THE CONTEXT OF INFORMATION SECURITY // Science Bulletin No. 7 (76), Volume 1. Pp. 614 - 618. 2024. ISSN 2712-8849 // Electronic resource: https://www.vesnik-nauki.rf/article/16689
4. Kodanev, I. A. Electronic digital signature and its application on the Unified Portal of State Services / I. A. Kodanev. - Text: direct // Young scientist. - 2023. - No. 23 (470). - P. 648-651. - URL: https://moluch.ru/archive/470/103897/ .
5. Van Dijk, J. and Jacobs, B. (2019). Electronic identification services as sociotechnical and political-economic constructs. *New Media and Society* , *22* (5), 896–914. https://doi.org/10.1177/1461444819872537
6. Komarova Antonina Vladislavovna, Menshchikov Alexander Alekseevich, Korobeynikov Anatoly Grigorievich Analysis and comparison of algorithms for electronic digital signature GOST R 34. 10-1994, GOST R 34. 10-2001 and GOST R 34. 10-2012 // Cybersecurity Issues. 2017. No. 1 (19). URL: https://cyberleninka.ru/article/n/analiz-i-sravnenie-algoritmov-elektronnoy-tsifrovoy-podpisi-gost-r-34-10-1994-gost-r-34-10-2001-i-gost-r-34-10-2012
7. Shchuka I. O., Nesterenko I. S., Nesterenko G. A. PROSPECTS, ADVANTAGES AND DISADVANTAGES OF ELECTRONIC SIGNATURE // MNIZH. 2023. No. 2 (128). URL: https://cyberleninka.ru/article/n/perspektivy-dostoinstva-i-nedostatki-elektronnoy-podpisi
8. Fursova E.A., Lazareva N.A. Coronacrisis: a problem for development or an incentive for digitalization of the economy? // Financial literacy in the context of the digital economy. St. Petersburg: SPbGUPTiD, 2022. P. 411-415
9. Searle J. Consciousness, Brain and Programs / trans. A. L. Blinov // URL: https://gtmarket.ru/library/articles/6661
10. Yatsutsenko V. V. Problems and prospects of introducing digital technologies into the activities of prosecutorial authorities // Actual problems of Russian law. - 2021. - Vol. 16. - No. 11 (132). - P. 187-193