Digital Identification from Smart Card to Digital Wallet –Eu Legal Framework and Situation in Bosnia and Herzegovina

Siniša Macan
Ministry of Interior of Republic of Srpska, BiH - sinisa.macan@mup.vladars.rs

Review paper

https://doi.org/10.7251/JIT2401037M UDC: 005.591.6:330.341(497.6)

Abstract: Information technologies and the entirely new digital world are experiencing significant development in the second and third decades of the twenty-first century. This development has led to the need to realize the concept of legal regulation of cyberspace, especially in the segment of digital identification. Digital identification is necessary to ensure security as well as the protection of personal data. Additionally, digital identification must guarantee the reliability and trust of signatories in the technologies used. The regulations adopted in previous years implied the existence of a PKI infrastructure and the storage of the private key by the signatory. However, the development of technologies and the widespread use of mobile and smart devices have generated the need for remote signing, cloud-based signing, and the creation of digital wallet techniques. It is precisely in this segment that the regulations have been amended. The paper presents EU regulations in this area and the situation in Bosnia and Herzegovina. It is particularly emphasized that the use of reliable legally grounded digital identification has not yet begun to be implemented in Bosnia and Herzegovina, and that it is necessary to establish practices and systems based on legal regulations that are aligned with the EU, as well as with the legal framework in Bosnia and Herzegovina.

Keywords: Digital identity, eID, digital wallet, eIDAS, eIDAS 2.0

Introduction

The real world and the digital world are closely integrated in the 21st century. The widespread use of digital devices, along with technological advancements, has completely blurred the boundaries between the physical, or real world on one side, and the digital world on the other. A vast number of human social activities, as well as trade, exchange of goods and services, and capital, have gained a completely new dimension with the development of information and communication technologies. Today, we don't just talk about technologies, but about an entirely new, information society. A society that operates in the real world and what is called cyberspace. In the last decade, the volume of retail through electronic commerce has increased by 3.2 times. The global volume of e-commerce in 2014 amounted to 1,336 billion US dollars, while in 2020 it increased to 4,280 billion US dollars, with a projected growth trend until 2023 to approximately 5,900 billion dollars. At the same time, statistics show that there are around 4.5 billion internet users worldwide, while approximately 3.8 billion people use social networks[1].

The cause of this state and these indicators are digital technologies that play a key role in almost every aspect of human life. Smartphones, portable devices, smart homes and vehicles, and a large number of other digital innovations have transformed the way people communicate, work, travel, shop, and even the way people socialize and engage in social interactions. The business world uses digital platforms for marketing, sales, and customer engagement, while industries such as healthcare, finance, and education embrace digital solutions to improve efficiency, accessibility, and the quality of services.

In the real, or physical world, rules of behavior have been introduced through the legal system and regulatory framework, as well as through moral and other societal norms. Data related to commodity exchange, as well as the number of Internet and social media users, unequivocally generate the need for appropriate attempts at regulation in cyberspace. This need is par-

ticularly pronounced in the adequate identification of individuals present in cyberspace, i.e., in the domain of establishing identity and access to the global network when conducting various types of transactions.

It is extremely important to establish a clear relationship between the real identity and the identity that an individual present in cyberspace when conducting electronic business, as well as when participating in global networks or various digital transactions. This type of identity is called digital identity.

Digital services that promote electronic business and commerce are one of the priorities of the European Union. Legislation related to digital identities, information security, and personal data protection is being significantly transformed in the European Union. The development of legislation is based on scientific and technological development, which is one of the foundations of the Treaty on the Functioning of the European Union.

In cyberspace, computer systems, mobile systems, a large number of sensors collecting data for so-called "smart systems," and large amounts of data are processed using artificial intelligence. "Cyberspace is a non-physical space where, according to current applicable legislation, there are no national borders and new rules are established based on the technical capabilities of computer systems." [2] "Cyberspace is a new type of space consisting of the Internet, World Wide Web,, i.e., basic infrastructure and information about the Internet and WWW, after the known and traditional four types of space: land, sea (ocean), airspace (atmospheric space, or internal space), and space. Cyberspace is actually the fifth space in which modern man lives, works, plays, and does business." [3]. Within cyberspace, and especially when conducting digital transactions that require reliability and security, mechanisms for verifying the identity of individuals must be provided.

Since 1999, when the first directive dealing with digital signatures was adopted, systems for digital identification have been established and used in member states, with problems of consistency and interoperability of systems arising between member states. The reform of regulations continued when Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) was adopted in 2014. Regulation eIDAS primarily established a legal basis for the establishment of an electronic identification and trust services system that would be unified and recognized equally in all European Union member states. Procedures were defined to ensure that through the accreditation process, the goal of ensuring that each trust service provider or certification body meets technical requirements in accordance with standards and recommendations is achieved. The accreditation process is carried out in a unified manner, guaranteeing uniform conditions throughout the territory of the European Union. Regulation 910/14 defines specific security levels, based on which the legal force of the electronic identification trust service, i.e., digital signature, is determined.

The development and widespread use of digital devices have led to the need for more precise definition of conditions for server signing, as well as for the use of digital means of identification, so Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, or eIDAS 2 regulation, was adopted in 2024. This regulation establishes an electronic wallet system, which enables the establishment of electronic documents in the electronic wallet in a reliable manner using trusted cryptographic mechanisms known only to the wallet owner. In addition, eIDAS regulation was related with Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

The Republic of Srpska, as well as Bosnia and Herzegovina, are in the process of integration with the European Union. The Stabilization and Association Agreement between the European Union, or its member states, on one side, and Bosnia and Herzegovina, on the other side, was signed in Luxembourg on June 16, 2008. The agreement entered into force on June 1, 2015. The Stabilization and Association Agreement is legally binding in Bosnia and Herzegovina and in the Republic of Srpska, so there is an obligation to harmonize regulations in BiH with the regulations of the European Union. The Republic of Srpska, as well as Bosnia and Herzegovina, have a legal obligation to harmonize their legislation with the legislation of the

European Union. This paper discusses the eIDAS and eIDAS 2 regulations, and presents the situation in the Republic of Srpska.

Digital Identity, Generaly

Digital identification, or digital ID, is the process of electronically verifying and authenticating the identity of individuals or entities in transactions and interactions that take place in cyberspace. In today's world, digital identification plays a crucial role in facilitating a wide range of online activities, including accessing digital services, conducting e-commerce, as well as participating in social networks and interacting with public administration.

As stated in the introductory chapter, digital identification systems are increasingly subject to legal regulation. They typically involve the use of unique identifiers, such as usernames, email addresses, or identification numbers, along with authentication mechanisms to verify the identity of users. These mechanisms can include passwords, Personal Identification Numbers - PINs, biometric data (such as fingerprints or facial recognition), cryptographic keys, or two-factor authentication (2FA), among others.

One of the key advantages of digital identification is its convenience and accessibility. Unlike traditional forms of identification, such as physical ID cards or passports, digital IDs can be easily accessed and used from any internet-enabled device, providing users with greater flexibility and mobility in their online interactions. This convenience is particularly important in situations where quick and secure access to digital services is essential, such as online banking, e-government services, or remote work environments.

Additionally, digital identification offers enhanced security and fraud prevention capabilities compared to traditional forms of identification. Advanced authentication methods, such as biometric authentication or cryptographic keys, can significantly reduce the risk of identity theft, phishing attacks, and unauthorized access to sensitive information. Furthermore, digital identification systems often incorporate encryption and other security measures to protect user data and privacy.

Digital identification also enables seamless and secure transactions and interactions across borders. In an increasingly globalized world, where individuals and companies routinely engage in international activities, the ability to verify identities in different jurisdictions is essential. Digital identification systems that adhere to international standards and interoperability protocols can facilitate cross-border trust and enable smooth international transactions.

Moreover, digital identification has the potential to promote financial inclusion and empower marginalized populations. In many parts of the world, a significant portion of the population lacks access to formal identification documents, which can hinder their ability to access financial services, healthcare, education, and other essential resources. Digital identification systems, especially those based on mobile technologies, offer a cost-effective and scalable solution to address this issue by providing individuals with a secure and verifiable means of identification.

However, despite its numerous advantages, digital identification also raises significant concerns regarding privacy, data security, and digital rights. One of the main concerns is the potential for misuse or improper use of personal data collected through digital identification systems. Inadequate safeguards and weak data protection measures can expose individuals to privacy violations, surveillance, identity theft, and other forms of abuse.

Furthermore, the centralized nature of many digital identification systems raises concerns about data security and the risk of single points of failure. Centralized databases containing sensitive personal information are attractive targets for hackers and cybercriminals, who may exploit vulnerabilities in the system to gain unauthorized access to user data. Additionally, the proliferation of digital identification systems raises questions about the concentration of power and control in the hands of governments or private entities that operate these systems.

Another challenge associated with digital identification is the issue of the digital divide and unequal access to technology. While digital identification has the potential to empower individuals and enhance their participation in the digital economy, disparities in access to technology, internet connectivity, and digital literacy can exacerbate existing inequalities and marginalize disadvantaged populations. Efforts to promote digital inclusion and bridge the digital divide are crucial to ensure that all individuals have equal opportunities to benefit from digital identification.

In response to these challenges, policymakers,

technologists, and civil society organizations are exploring ways to design and implement digital identification systems that prioritize privacy, security, and user empowerment. Principles such as privacy by design, data minimization, user consent, transparency, and accountability are increasingly being integrated into the design and governance of digital identification systems to mitigate risks and protect user rights.

Moreover, decentralized identity technologies, such as self-sovereign identity (SSI) systems based on blockchain or distributed ledger technology (DLT), offer promising alternatives to centralized digital identification systems. By giving individuals greater control over their personal data and reducing reliance on intermediaries, decentralized identity solutions can enhance privacy, security, and user autonomy in digital interactions.

In conclusion, digital identification is a key enabler of the digital economy and society, offering numerous benefits in terms of convenience, security, and inclusivity. However, realizing the full potential of digital identification requires addressing significant challenges related to privacy, security, and digital rights. By adopting principles of privacy, security, and user empowerment, as well as leveraging emerging technologies such as decentralized identity, stakeholders can create digital identification systems that are secure, reliable, and respectful of individual rights and freedoms.

EU REGULATION

eIDAS Regulation (Regulation (EU) No 910/2014) is a fundamental piece of legislation in the European Union (EU) that aims to establish a framework for electronic identification and trust services for electronic transactions in the internal market. The regulation provides a legal foundation for secure and seamless electronic interactions between businesses, citizens, and public authorities across EU member states.

The eIDAS Regulation, which stands for "electronic IDentification, Authentication, and trust Services," is a significant piece of legislation in the European Union (EU) aimed at facilitating secure and seamless electronic transactions across member states. Enacted in 2014, eIDAS replaced the previous Electronic Signature Directive (1999/93/EC) and established a comprehensive legal framework for electronic identification and trust services within the EU. This article provides a detailed examination of the eIDAS Regulation, its objectives, key provisions, implementation challenges, and the implications for businesses and individuals.

The primary objectives of the eIDAS Regulation are to enhance trust and security in electronic transactions, promote the use of electronic identification (eID) and electronic signatures, and facilitate cross-border recognition of electronic trust services within the EU. By establishing uniform standards and legal requirements for electronic identification and trust services, eIDAS aims to create a digital single market where businesses and citizens can engage in electronic transactions with confidence and convenience.

Key Provisions of eIDAS

Electronic Identification (eID): eIDAS defines electronic identification as the process of uniquely identifying individuals or legal entities in electronic transactions. Member states are required to establish and maintain electronic identification schemes that meet specified criteria, including security, reliability, and interoperability. Qualified electronic identification (QeID) schemes, which comply with additional requirements, are granted a higher level of legal recognition across the EU.

Electronic Signatures: eIDAS recognizes various types of electronic signatures, including simple electronic signatures, advanced electronic signatures (AdES), and qualified electronic signatures (QES). AdES and QES are subject to specific requirements regarding authenticity, integrity, and non-repudiation. QES, in particular, provides the highest level of legal certainty and is equivalent to a handwritten signature under EU law.

Trust Services: eIDAS establishes a framework for electronic trust services, such as electronic seals, electronic time stamps, electronic registered delivery services (ERDS), and website authentication certificates. Trust service providers (TSPs) must adhere to strict requirements concerning security, liability, and transparency. Qualified trust service providers (QTSPs) undergo a rigorous certification process to ensure compliance with eIDAS standards.

Cross-Border Recognition: One of the key objectives of eIDAS is to enable seamless cross-border recognition of electronic identification and trust services within the EU. Member states are required to recognize electronic signatures, electronic seals, electronic documents, and other trust services issued

by qualified providers in other EU countries. This facilitates the expansion of digital business activities across borders and reduces administrative barriers for citizens and businesses operating in the EU.

Implementation Challenges

While eIDAS represents a significant step towards harmonizing electronic identification and trust services across the EU, its implementation has posed several challenges for member states and stakeholders. Some of the key challenges include:

Technical interoperability: Ensuring seamless interoperability between different national eID schemes and trust service infrastructures remains a complex task, requiring standardization and compatibility efforts.

Legal harmonization: Achieving uniform interpretation and application of eIDAS provisions across member states' legal systems requires ongoing coordination and cooperation among national authorities and judicial bodies.

User acceptance: Encouraging widespread adoption of electronic identification and trust services among citizens, businesses, and public administrations requires awareness-raising campaigns, user-friendly interfaces, and effective communication strategies.

Security and privacy concerns: Addressing concerns related to data security, privacy protection, and cybersecurity threats is essential to maintaining trust in electronic transactions and preventing fraud or misuse of electronic identities and signatures.

Implications for Businesses and Individuals

The eIDAS Regulation has significant implications for businesses, governments, and individuals operating within the EU. For businesses, eIDAS offers opportunities to streamline administrative processes, reduce costs, and expand market reach by leveraging electronic identification and trust services. Qualified trust service providers can offer innovative solutions for electronic authentication, document signing, and secure communication, enhancing business efficiency and competitiveness. For individuals, eIDAS provides greater convenience and accessibility in accessing digital services, conducting online transactions, and interacting with public authorities across borders. By enabling secure and reliable electronic identification and signature solutions, eIDAS empowers citizens to participate more actively in the digital economy and exercise their rights in a digitalized society.

The eIDAS Regulation represents a significant milestone in the development of a harmonized legal framework for electronic identification and trust services within the European Union. By establishing common standards, promoting interoperability, and fostering trust in electronic transactions, eIDAS aims to facilitate the digital transformation of businesses and public services, enhance cross-border cooperation, and empower citizens in the digital age. While challenges remain in terms of technical implementation, legal harmonization, and user acceptance, eIDAS lays the foundation for a more secure, efficient, and inclusive digital single market in Europe

eIDAS 2

In recent years, there have been discussions and proposals for an updated version of the eIDAS regulation, often referred to as "eIDAS 2." While eIDAS has laid a solid groundwork for electronic identification and trust services, technological advancements, evolving digital needs, and emerging security threats have prompted calls for revisions and enhancements to ensure the regulation remains relevant and effective in the rapidly changing digital landscape.

eIDAS 2 is envisioned as a comprehensive update to the existing regulation, aiming to address existing shortcomings, incorporate new technological developments, and strengthen the trust framework for electronic transactions. The proposed amendments and additions under eIDAS 2 are expected to shape the future of digital identity management and electronic trust services within the EU.

One of the key aspects of eIDAS 2 is the expansion of the scope of the regulation to cover a broader range of electronic services and transactions. This includes provisions for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, website authentication, and electronic identification (eID) schemes. By encompassing a wider array of digital services, eIDAS 2 seeks to facilitate greater interoperability and cross-border acceptance of electronic transactions within the EU.

Furthermore, eIDAS 2 aims to address interoperability challenges that hinder seamless cross-border

recognition of electronic identities and trust services. Interoperability is crucial for enabling citizens and businesses to use their electronic identities and trust services across different member states without encountering unnecessary barriers. To achieve this goal, eIDAS 2 may introduce standardized protocols, technical specifications, and interoperability frameworks to ensure compatibility and harmonization of electronic identification systems and trust services across the EU.

Additionally, eIDAS 2 is expected to place a stronger emphasis on security and privacy aspects of electronic identification and trust services. With the increasing prevalence of cyber threats and data breaches, ensuring the confidentiality, integrity, and authenticity of electronic transactions is paramount. eIDAS 2 may introduce stricter security requirements, robust authentication mechanisms, encryption standards, and data protection measures to enhance the overall trustworthiness and resilience of electronic systems and services.

Moreover, eIDAS 2 may introduce provisions to foster innovation and adoption of emerging technologies in the field of electronic identification and trust services. This includes support for technologies such as blockchain, biometrics, artificial intelligence, and machine learning, which have the potential to revolutionize the way electronic identities are managed and verified. By embracing innovation, eIDAS 2 aims to future-proof the regulation and ensure its relevance in the rapidly evolving digital landscape.

Another key aspect of eIDAS 2 is the reinforcement of legal certainty and cross-border recognition of electronic signatures and other trust services. Cross-border recognition is essential for promoting cross-border trade, e-commerce, and digital collaboration within the EU. eIDAS 2 may introduce mechanisms to streamline the mutual recognition of electronic signatures and trust services across member states, thereby reducing administrative burdens and legal uncertainties associated with cross-border electronic transactions.

Furthermore, eIDAS 2 may introduce provisions to strengthen consumer protection and user rights in the context of electronic identification and trust services. This includes transparency requirements, user consent mechanisms, recourse mechanisms, and liability frameworks to ensure that consumers are adequately informed and empowered when using electronic services. By safeguarding consumer rights, eIDAS 2 aims to build trust and confidence in electronic transactions and foster greater uptake of digital services among citizens and businesses.

In conclusion, eIDAS 2 represents a significant milestone in the ongoing evolution of electronic identification and trust services within the EU. By addressing key challenges, embracing technological innovation, and strengthening the legal and technical framework for electronic transactions, eIDAS 2 aims to facilitate secure, seamless, and trusted electronic interactions across member states. As digitalization continues to reshape the economy and society, eIDAS 2 is poised to play a central role in unlocking the full potential of the digital single market and driving Europe's digital transformation agenda forward.

Personal data protection

In the digital landscape, two fundamental regulations play a pivotal role in shaping the way data is handled and identities are verified: the General Data Protection Regulation (GDPR) and the Electronic Identification, Authentication and Trust Services Regulation (eIDAS). While they serve distinct purposes, these regulations are closely intertwined, working together to safeguard individuals' privacy, ensure data security, and foster trust in digital interactions.

The General Data Protection Regulation (GDPR), implemented in May 2018, is a comprehensive data protection framework applicable to all entities processing personal data of individuals residing in the European Union (EU). It aims to harmonize data protection laws across EU member states, empower individuals with greater control over their personal data, and establish accountability and transparency requirements for organizations handling such data.

Key principles of GDPR include:

- Lawfulness, Fairness, and Transparency: Data processing must be lawful, fair, and transparent to the data subjects.
- Purpose Limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Data Minimization: Data controllers must ensure that personal data processed is adequate, relevant, and limited to what is necessary.
- Accuracy: Personal data must be accurate and,

where necessary, kept up to date.
- Storage Limitation: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary.
- Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage.

Non-compliance with GDPR can result in severe penalties, including fines of up to €20 million or 4% of the annual global turnover, whichever is higher.

While GDPR focuses primarily on data protection and privacy, and eIDAS centers on electronic identification and trust services, the two regulations intersect in several areas:
- Data Protection in eIDAS Transactions: eIDAS mandates that trust service providers adhere to stringent security measures to protect personal data processed during electronic transactions. These security requirements align closely with GDPR's principles of data protection by design and default.
- Legal Validity of Electronic Signatures: eIDAS establishes a legal framework for electronic signatures, including qualified electronic signatures, which hold the same legal validity as handwritten signatures. GDPR recognizes the use of electronic signatures for obtaining consent and executing contracts, provided they meet the criteria outlined in eIDAS.
- Authentication and Authorization: Both regulations emphasize the importance of ensuring secure authentication and authorization mechanisms to protect individuals' personal data. eIDAS provides the framework for electronic identification, while GDPR sets forth requirements for obtaining explicit consent and implementing appropriate security measures.
- Cross-border Data Transfers: eIDAS facilitates cross-border recognition of electronic identification and trust services, enabling seamless digital interactions between EU member states. GDPR's provisions on international data transfers apply to personal data exchanged during such transactions, ensuring that data protection standards are upheld regardless of geographical boundaries.

In today's digital era, the harmonious implementation of GDPR and eIDAS as well as eIDAS 2.0 is crucial for fostering trust, ensuring data protection, and facilitating secure electronic transactions within the EU. By adhering to the principles outlined in both regulations and leveraging the synergies between them, organizations can navigate the complexities of digital identity management while safeguarding individuals' privacy rights and promoting digital innovation and growth.

Legal Framework in Bosnia and Herzegovina

The legislation of Bosnia and Herzegovina, although incompetent for the area of digital signatures and certificates, adopted the Law on Electronic Signature of Bosnia and Herzegovina in 2006 ("Official Gazette of BiH" No. 91/06). The Law on Electronic Signature of Bosnia and Herzegovina is harmonized with Directive 1999/93/EC on a Community framework for electronic signatures. The BiH Law is not harmonized with Regulation No. 910/14 on electronic identification and trust services for electronic transactions on the internal market (hereinafter: eIDAS).

The BiH Law is in force and fully applied with unfavorable solutions for Republika Srpska. According to this law, the Office for Supervision and Accreditation of Certifiers has been established within the Ministry of Communications and Transport, which fully performs its function in accordance with this Law. The accreditation procedure is conducted, and a Register of Certifiers is maintained, which currently includes three legal entities (Halcom D.D. Ljubljana, registered on October 3, 2019, the Indirect Taxation Authority based in Banja Luka, registered on May 12, 2021, and the Agency for Identification Documents, Records, and Data Exchange of Bosnia and Herzegovina, based in Banja Luka, registered on April 15, 2022). The Ministry of Communications and Transport of Bosnia and Herzegovina is recognized as the Supervisory Authority on behalf of Bosnia and Herzegovina in the Forum of European Supervisory Authorities for Trust Service Providers (FESA), as well as competent to maintain the list of trust service providers. Trust service providers and digital identity providers registered in the registers maintained by the Supervisory Authority of BiH are visible beyond the borders of Bosnia and Herzegovina, i.e., on the EU market.

In the parliamentary procedure at the BiH level, there was a proposal for the Law on Electronic Iden-

tification and Trust Services for Electronic Transactions of Bosnia and Herzegovina No. 01.02-02-1-667/19, dated March 26, 2019, which was rejected. It is undeniable that the issue of digital identification needs to be regulated, but solely in accordance with constitutional competencies.

At the level of the Federation of Bosnia and Herzegovina, a regulation on electronic signatures has not been adopted, but the Law on Electronic Document ("Official Gazette of FBiH" 55/13) has been adopted.

LEGAL FRAMEWORK IN REPUBLIC OF SRPSKA

The area of digital identification and the application of digital identities in Republika Srpska is regulated by the following legal regulations:

- Law on Electronic Signature of Republika Srpska ("Official Gazette of Republika Srpska", No. 106/15 and 83/19), with corresponding subordinate regulations.
- Law on Electronic Document ("Official Gazette of Republika Srpska", No. 106/15).
- Law on Electronic Business of Republika Srpska ("Official Gazette of Republika Srpska", No. 59/09 and 33/16).
- Law on the Agency for Information and Communication Technologies ("Official Gazette of Republika Srpska" No. 102/23).

According to the above, the legal framework in Republika Srpska enables the immediate use of trust services of digital identification, defines schemes of digital identification, and allows legal entities, especially the business community, to use current qualified or unqualified digital certificates. E-government, as a significant actor in overall electronic business, can currently provide trust services according to identification schemes.

Key procedures related to trust services are:

- Procedure for prescribing conditions for the operation of CA bodies.
- Accreditation procedure and compliance verification of CA bodies.
- Maintenance of the CA body register, which is publicly available.
- Supervision procedure over the work of CA bodies.

Establishment of identification schemes and registers of service providers of various identification schemes.

In Republika Srpska, the Regulation on Special Conditions that CA bodies must meet ("Official Gazette of Republika Srpska" No. 78/16 and 108/19) prescribes the conditions that CA bodies must meet.

The accreditation procedure in Republika Srpska is regulated according to Article 22 of the Law on Digital Signature, which allows any legal entity intending to issue qualified digital certificates to carry out this activity based on a permit from the relevant ministry. A request for a permit to operate as a certification body is submitted to the Ministry of Administration and Local Self-Government. Based on the request, the Minister forms a Commission for Compliance Verification. After the procedure, the qualified certification body is entered in the register of certification bodies of Republika Srpska, which is publicly available. This procedure is not harmonized with the eIDAS regulation and is not transparent enough.

Related to the previous regulations of Republika Srpska, the use of electronic signatures and qualified electronic signatures is defined, and two types of records are kept, which opens the possibility for the application of eIDAS identification schemes and the current beginning of the application of the Law on Electronic Signature in certain areas. In the records of unqualified bodies maintained by the Ministry of Scientific and Technological Development and Higher Education on May 2024, three legal entities are registered: Ministry of Administration and Local Self-Government of Republika Srpska, the Tax Administration of Republika Srpska, and Sberbank a.d. Banja Luka. The MF Bank is also registered, but this information is not publicly available in the register.

According to Article 34, supervision over the implementation of the Law is carried out by the Republic Administration for Inspection Affairs.

Republic of Srpska as well as Bosnia and Herzegovina legaly not recognized requirenmants from eIDAS 2 regulation.

CONCLUSION

The state of digital identification in the Republic of Srpska presents a multifaceted landscape, shaped by various factors including regulatory frameworks, technological infrastructure, adoption rates, challenges, and ongoing initiatives. This analysis provides an overview of the current state of digital identification in Republic of Srpska, highlighting key aspects and potential pathways for improvement.

Republic of Srpska has established a legal framework for digital identification, primarily governed by laws related to electronic signatures, electronic documents, and electronic business. The Law on Electronic Signature of Republic of Srpska, in line with national legislation, provides a foundation for electronic authentication and signature mechanisms. Additionally, regulations pertaining to electronic documents and electronic business further support digital identification practices within Republic of Srpska. In 2023, the Republic of Srpska finally adopted the Law on the Agency for Information and Communication Technologies, thereby establishing an institution responsible for digital identification as well as information security.

The technological infrastructure supporting digital identification in Republic of Srpska is evolving, with efforts to modernize and enhance existing systems. Public Key Infrastructure (PKI) systems are utilized for secure authentication and digital signatures, facilitating electronic transactions and communications. However, there may be gaps in the coverage and interoperability of digital identification systems across different sectors and entities within RS.

The adoption of digital identification solutions in Republic of Srpska varies across different segments of society and industries. While government agencies and certain sectors may have implemented digital identification mechanisms, there may be disparities in adoption rates among businesses, organizations, and individuals. Factors influencing adoption include awareness, accessibility, ease of use, and trust in digital technologies.

Several challenges exist in advancing digital identification in Republic of Srpska:

- Regulatory Compliance: Ensuring compliance with national and international regulations, including EU standards such as the eIDAS Regulation, poses a challenge. Harmonizing RS's legal framework with evolving regulatory requirements necessitates continuous updates and amendments to existing laws and regulations.
- Infrastructure Development: Enhancing the technological infrastructure for digital identification, including PKI systems, authentication mechanisms, and interoperable platforms, requires investments in infrastructure development and technology upgrades. This entails addressing infrastructure gaps, ensuring scalability, and fostering interoperability across systems.
- Data Privacy and Security: Addressing concerns related to data privacy, security vulnerabilities, and identity theft is essential for building trust and confidence in digital identification systems. Implementing robust data protection measures, encryption protocols, and cybersecurity standards is crucial to safeguarding personal information and mitigating risks.
- Awareness and Education: Promoting awareness and understanding of digital identification among stakeholders, including citizens, businesses, and government agencies, is vital for increasing adoption rates and fostering trust in digital technologies. Educational initiatives, training programs, and outreach campaigns can help raise awareness about the benefits and functionalities of digital identification.

To address these challenges and improve the state of digital identification in Republic of Srpska, several strategies can be considered:

- Regulatory Reforms: Enhance the legal framework for digital identification by aligning with international standards and best practices, including the eIDAS and eIDAS 2 Regulation. This involves revising existing laws, adopting new regulations, and ensuring compliance with evolving regulatory requirements.
- Infrastructure Investments: Invest in upgrading and modernizing the technological infrastructure for digital identification, including PKI systems, authentication protocols, and interoperable platforms. This requires strategic investments in infrastructure projects, technology upgrades, and capacity building initiatives.
- Data Protection Measures: Strengthen data privacy and security measures to protect personal information and mitigate cybersecurity risks. This includes implementing robust encryption standards, adopting cybersecurity best practices, and conducting regular audits and assessments to identify and address vulnerabilities.
- Awareness Campaigns: Launch targeted awareness campaigns to educate stakeholders about the benefits, functionalities, and security features of digital identification. This involves disseminating informative materials, organizing workshops and seminars, and engaging with

key stakeholders to address concerns and misconceptions.
- Intersectoral Collaboration: Foster collaboration and cooperation among government agencies, regulatory bodies, industry associations, academia, and civil society organizations to develop coordinated approaches and share best practices. This includes establishing intersectoral working groups, promoting information exchange, and fostering a culture of collaboration and innovation.

By implementing these strategies and fostering a conducive environment for digital innovation and transformation, the Republic of Srpska can enhance its digital identification capabilities, promote economic growth, and improve the delivery of public services in the digital age.

REFERENCES

[1] Macan, S, Sajber pravo i pravni aspekti sajber prostora, Panevropski univerzitet Apeiron, Banja Luka, 2022

[2] Macan, S, Specificity of design of information systems for identification of citizens, master thesis, FON, Belgrade, 2006

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

[4] Parliamentary Assembly of Bosnia and Herzegovina, Law on Protection of Personal Data („Official Gazette of Bosnia and Herzegovina" 49/06, 76/11 and 89/11)

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

[6] Nogo, S., & Macan, S. eServices Platform. Beograd: SMART eGovernment 2009.

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

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

[9] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), 2014

[10] Cohen, J. E., Cyberspace As/And Space, Georgetown University Law Center, 2007

[11] Windley, P. J. Understanding Digital Identity Managament. The Windley Group, 2003

[12] Song, Y.Y, Cybercryptography: Applicable Cryptography for Cyberspace Security, ISBN 978-3-319-72534-5, Springer Nature Switzerland, https://doi.org/10.1007/978-3-319-72536-9, 2019

[13] Dijck, J. V., Jacobs, B., Electronic identity services as sociotechnical and political-economic constructs, Vol. 22(5) 896–914, New media and sociati, Sage, DOI: 10.1177/1461444819872537, 2020

[14] Macan, S. (Juli 2020). Procjena usklađenosti u postupku primjene zakona o digitalnom potpisu Republike Srpske i usaglašenost sa eIDAS regulativom. Banja Luka: Godišnjak Fakulteta pravnih nauka, broj 10, UDC: 340.132.6:349.412, pp. 241-255.

[15] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

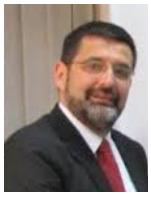
[16] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[17] Digitalna identifikacija i nivoi bezbednosti elektronskih potpisa, ITEO 2022, XIV međunarodni naučno-stručni skup Informacione tehnologije za e-obrazovanje, Panevropski univerzitet "APEIRON", Banja Luka, godina 2022.

[18] www.europe.eu

Received: May 9, 2024
Accepted: May 16, 2024

ABOUT THE AUTHORS



Sinisa Macan, assistant professor is an advisor in the ICT Department of the Ministry of Interior of the Republic of Srpska, with extensive experience in top and mid-level management positions in the ICT field. He graduated from the Faculty of Organizational Sciences at the University of Belgrade. He earned his Master's degree in Technical Sciences – Information Systems in 2006 from the same faculty at the University of Belgrade, and defended his doctoral dissertation in 2018 in Banja Luka. From 2006 to 2009, he was the director of the CIPS Directorate, and from 2009 to 2015, he was the first director and proposer for the establishment of IDDEEA, the agency responsible for ID documents and record keeping. His work at IDDEEA was crucial in obtaining visa-free travel with Schengen Agreement countries. He is currently a member of the Board of Directors of the ICT Agency of the Republic of Srpska and teaches Cyber Law as an assistant professor. He has participated in the following projects: the CIPS project (establishment of the citizen registry system, personal documents, and driver's licenses in Bosnia and Herzegovina), the passport and electronic passport system, passive voter registration in Bosnia and Herzegovina, the data transmission network for public security authorities, the vehicle registration system, etc. In 2011, the European Movement in Bosnia and Herzegovina awarded him the title "The Most European of Bosnia and Herzegovina for 2011."

FOR CITATION

Siniša Macan, Digital Identification from Smart Card to Digital Wallet –Eu Legal Framework and Situation in Bosnia and Herzegovina, *JITA – Journal of Information Technology and Applications, Banja Luka*, Pan-Europien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 14(2024)1:37-46, (UDC: 005.591.6:330.341(497.6)), (DOI: 10.7251/JIT2401037M, Volume 14, Number 1, Banja Luka, June (1-88), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004