Revista JURÍDICA PORTUCALENSE

www.upt.pt

Nº 38 | Universidade Portucalense | Porto | 2025

https://doi.org/10.34625/issn.2183-2705(38)2025

Oleh PREDMESTNIKOV, Tetyana KAGANOVSKA, Iryna PAKHOMOVA, Anastasiia OREL, Kateryna ROHOZINNIKOVA

Administrative and Legal Regulation of the Electronic Identification of Citizens

DOI: https://doi.org/10.34625/issn.2183-2705(38)2025.ic-21

Secção

Investigação Científica / Scientific Research*

* Os artigos presentes nesta secção foram sujeitos a processo de revisão segundo o método *blind peer review* / The articles in this section have undergone a blind peer review process.

Administrative and Legal Regulation of the Electronic Identification of Citizens

Regulamentação Administrativa e Jurídica da Identificação Eletrónica dos Cidadãos

Oleh PREDMESTNIKOV[1]
Tetyana KAGANOVSKA[2]
Iryna PAKHOMOVA[3]
Anastasiia OREL[4]
Kateryna ROHOZINNIKOVA[5]

ABSTRACT: The relevance of studying the administrative and legal regulation of electronic identification in Ukraine arises from the rapid digitalisation of public services and the inconsistency of national legislation with international standards. This study aims to identify gaps in the legal framework and propose mechanisms for its harmonisation with the eIDAS Regulation and related technical standards. The methodology combines theoretical and legal analysis of Ukrainian and EU legislation, examination of six judicial decisions of the Supreme and Constitutional Courts of Ukraine, content analysis of institutional reports from the Ministry of Digital Transformation, the National Bank of Ukraine, SE "Diia", and the Central Certification Authority, as well as comparative legal analysis of the legislation of Poland, Lithuania, Estonia, Germany, France, and the United States. The findings demonstrate systemic fragmentation of Ukraine's legal framework, insufficient legal recognition of BankID and MobileID, and a lack of alignment with international assurance levels. The study proposes amendments to the Law "On Electronic Trust Services", the introduction of a unified QES verification procedure, and the mapping of national assurance levels to eIDAS standards. The scientific novelty lies in integrating legal, institutional, and technical perspectives to develop draftable recommendations for modernising Ukraine's digital identification system.
KEYWORDS: Electronic Identification; Digital Identity; Administrative and Information Law of Ukraine; eIDAS Regulation; Judicial Interpretation; Cross-Border Authentication; Data Protection.

RESUMO: A relevância do estudo sobre a regulação administrativa e jurídica da identificação eletrónica na Ucrânia decorre da rápida digitalização dos serviços públicos e da incoerência da legislação nacional com as normas internacionais. O objetivo da pesquisa é identificar lacunas no quadro jurídico e propor mecanismos para a sua harmonização com o Regulamento eIDAS e as normas técnicas associadas. A metodologia combina a análise

[1] Doctor of Legal Sciences, Professor, Head of the Department of Law, Faculty of Natural Sciences and Geography, Bogdan Khmelnitsky Melitopol State Pedagogical University, Zaporizhzhia, Ukraine; email olehpredmestnikov.melitopol@gmail.com; ORCID: 0000-0001-8196-647X
[2] Doctor of Law, Professor of the Department of State and Legal Disciplines, Faculty of Law, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine; email: tetianatrshch@gmail.com; ORCID: 0000-0002-4427-2038
[3] Candidate of Law, Associate Professor of the Department of State and Legal Disciplines, Faculty of Law, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine; email: irynazvarych12@gmail.com; ORCID: 0000-0001-6221-5902
[4] PhD Student in Law, Interregional Academy of Personnel Management, Kyiv, Ukraine; email ok228b@gmail.com; ORCID: 0009-0008-9804-105X
[5] Candidate of Juridical Sciences, Associate Professor of the Department of Law Enforcement Activities and Special Legal Disciplines, Educational-Scientific Institute of Law, National University of Water Management and Environmental Engineering, Rivne, Ukraine; email: katerynal73196@gmail.com; ORCID: 0000-0003-2866-408X

teórico-jurídica da legislação ucraniana e europeia, o exame de seis decisões dos Tribunais Supremo e Constitucional da Ucrânia, a análise de conteúdo dos relatórios institucionais do Ministério da Transformação Digital, do Banco Nacional da Ucrânia, da Empresa Estatal "Diia" e da Autoridade Central de Certificação, bem como uma análise jurídica comparativa da legislação da Polónia, Lituânia, Estónia, Alemanha, França e Estados Unidos. Os resultados revelam fragmentação sistémica do quadro jurídico ucraniano, ausência de reconhecimento legal do BankID e do MobileID e falta de alinhamento com os níveis de garantia internacionais. O estudo propõe alterações à Lei "Sobre os Serviços de Confiança Eletrónicos", a introdução de um procedimento unificado de verificação de QES e o mapeamento dos níveis nacionais de garantia com os padrões do eIDAS. A novidade científica reside na integração dos aspetos jurídicos, institucionais e técnicos, oferecendo recomendações normativas para a modernização do sistema de identificação digital da Ucrânia.
Palavras-chave: Identificação Eletrónica; Identidade Digital; Direito Administrativo e da Informação da Ucrânia; Regulamento eIDAS; Interpretação Judicial; Autenticação Transfronteiriça; Proteção de Dados.

1. Introduction

The digital transformation of public administration and services in Ukraine requires secure and legally valid electronic identification (eID). However, Ukraine's legal framework remains fragmented and only partially aligned with the eIDAS Regulation (EU) 2024/1183, despite the widespread use of BankID, MobileID, and Diia.Signature. This inconsistency complicates the protection of digital rights and results in divergent judicial interpretations of authentication and signature mechanisms. Improving the system demands harmonisation with European and international standards, the development of coherent judicial practice, and the adoption of technically verified identification models. The study focuses on legal and technical aspects, particularly digital identity infrastructure, data protection, certification, and case law related to electronic authentication.

Despite several reforms, systemic challenges persist–contradictions between key laws, insufficient regulation of private identification methods, and unclear administrative procedures for verifying digital credentials. The study therefore aims to identify regulatory gaps and propose improvements based on judicial practice, comparative experience, and modern standards.

Research objectives:

- Analyse the legal framework for eID in Ukraine and identify its key inconsistencies.

- Examine court decisions on electronic signatures, documents, and digital identity.

- Compare foreign models of e-identification and evaluate their applicability in Ukraine.

The findings support the development of a coherent and legally sound model of electronic identification, ensuring trust and protection of citizens' rights in the digital environment.

2. Literature Review

A review of the academic literature on digital identification in public law shows a wide range of approaches to defining the legal status of a digital identity, the boundaries of government intervention, and authentication processes. The perspective of Macan, who highlights that technical reliability alone is insufficient without proper legal support, aligns perfectly with our analysis of domestic legislation.[6] Our study found an apparent disconnect between existing technical solutions (like MobileID and BankID) and their regulation in law.

On the other hand, the perspective of Dagiral and Singh, which frames digital identification as a political tool for managing citizenship and potentially excluding certain groups, has partial relevance in Ukraine.[7] In particular, where vulnerable populations have limited access to digital tools, there is a risk of violating the principle of equal access to public services. This highlights the need to account for the socio-legal context when designing authentication systems.

Subramanian continues this critical line of inquiry, pointing to the risks of unified digital identifiers in states with a multi-component ethnic or caste composition.[8] The author contends that excessive standardisation of digital identity can negate the principles of inclusion and justice, particularly in states with low institutional trust. In contrast, Alonso argues for the expediency of expanding the functionality of the eIDAS system by incorporating academic attributes.[9] In his view, this would not only enhance

[6] MACAN, Siniša. Legal acceptability of the security level of the electronic identification system. *Godišnjak Fakulteta Pravnih Nauka,* 2021, vol. 11, no. 11, pp. 186-199. https://doi.org/10.7251/gfp2111186m

[7] DAGIRAL, Eric and SINGH, Khertimayum. Governance and accountable citizenship through identification infrastructures: Database politics of Copernicus (France) and National Register of Citizens (India). *Science, Technology and Society*, 2020, vol. 25, no. 3, pp. 368-385. https://doi.org/10.1177/0971721820912895

[8] SUBRAMANIAN, Vidya. Citizenship in India: Parsing the complexity of digital identity systems. *Science, Technology and Society*, 2024, vol. 29, no. 4, pp. 595-613. https://doi.org/10.1177/09717218241281940

[9] ALONSO, Álvaro, et al. Enhancing university services by extending the eIDAS European specification with academic attributes. *Sustainability*, 2020, vol. 12, no. 3, 770. https://doi.org/10.3390/su12030770

the universality of identification but also promote its effectiveness in the cross-border educational-administrative environment.

Approaching the issue from a legal positivist perspective, Chiang and Hoesin assert that integrating artificial intelligence into unified ID systems is legally acceptable only if its use is clearly defined by law.[10] The authors stress that without a proper legislative framework, these systems risk violating the principles of personal autonomy and equality before the law.

Páez et al. proposed a blockchain model for biometric documents, which entails the decentralised storage of identification information.[11] Such an approach ensures a higher level of transparency and individual control. Still, it raises doubts among legal scholars regarding the stability of legal interactions in a decentralised environment. Golić emphasises precisely this point, indicating the experience of Serbia, where decentralisation without corresponding legislative updates creates legal uncertainty in the sphere of electronic administration.[12]

Sudiarawan et al. emphasise the contradictions between the norms of administrative and procedural legislation in the context of the use of digital evidence.[13] Their conclusion regarding the absence of unified standards for the admissibility of electronic documents in judicial proceedings is entirely consistent with the results of the analysis of Ukrainian practice conducted herein. In turn, the position of Correa-Marichal et al., who criticise the architecture of the electronic identity card in Spain due to technical vulnerabilities and a lack of transparency in its administration, partially correlates with the conclusions regarding the Ukrainian context.[14]

Amorim et al. emphasise that the effectiveness of electronic identification is contingent upon the existence of a clear legal environment, technical audits, and

[10] CHIANG, Daud and HOESIN, Zainal. Ensuring equality before the law and personal data protection through implementation of AI integration in single identification number systems: A positivist philosophy perspective. *Devotion - Journal of Research and Community Service,* 2024, vol. 5, no. 11, pp. 1347-1361. https://doi.org/10.59188/devotion.v5i11.20688

[11] PÁEZ, Rafael, et al. An architecture for biometric electronic identification document system based on blockchain. *Future Internet*, 2020, vol. 12, no. 1, 10. https://doi.org/10.3390/fi12010010

[12] GOLIĆ, Darko. Normative regulation of electronic administration in the Republic of Serbia. *Pravo - Teorija i Praksa*, 2023, vol. 40, pp. 44-62. https://doi.org/10.5937/ptp2300044g

[13] SUDIARAWAN, Kadek, et al. Discourses on citizen lawsuit as administrative dispute object: Government administration law vs. administrative court law. *Journal of Indonesian Legal Studies,* 2022, vol. 7, no. 2, pp. 499-486. https://doi.org/10.15294/jils.v7i2.60166

[14] CORREA-MARICHAL, Javier, et al. Study and security analysis of the Spanish identity card. *Cryptography and Security,* 2022. https://doi.org/10.48550/arXiv.2210.04064

transparent accountability for data processing.[15] This position is entirely consistent with the problems identified in this study - namely, the lack of normative detail in the control mechanisms for digital transactions and the limited accountability of identification service operators. Both cases point to the danger of centralising digital power without sufficient legal constraints.

The position of Afdhal also corroborates the study's conclusions regarding the risks inherent in identification systems under conditions of fragmented regulation. [16] In the context of Ukrainian practice, similar threats are manifested in the form of ambiguous guarantees of the right to the rectification or erasure of personal data, as well as the absence of mechanisms for the adequate protection of citizens' rights during the processing of information in digital registries.

3. Materials and Methods

The study of administrative and information law regulation of electronic identification of citizens was carried out in three stages. Its goal was to identify gaps in the regulatory framework, evaluate judicial enforcement, and compare foreign approaches to organising electronic identification. Particular attention was given to the interaction between public systems (Diia, MobileID, BankID) and private infrastructure providers ensuring access to digital services.

The first stage involved a theoretical-legal analysis of Ukrainian and EU legislation and analytical reports from ENISA, OECD, and ITU. Seven key instruments were reviewed: the Law of Ukraine “On Electronic Trust Services”, the Law “On Personal Data Protection”, resolutions of the Cabinet of Ministers, regulations of the NBU and MDT, the Regulation (EU) 2024/1183 (eIDAS 2.0), ISO/IEC 24760-1:2019 + Amd 1:2023, and NIST SP 800-63 Rev. 4 (2024). These normative and technical acts are listed in Annex I (Legislative Acts Analysed) with full titles and official sources, rather than in the References section. The assessment focused on their hierarchy, correlation, and alignment with international norms.

The second stage comprised an empirical analysis of judicial practice. It

[15] AMORIM, Joni A., DE SIQUERIA ROCHA, Jose and MAGAL-ROYO, Teresa. Cybersecurity in Europe: Digital identification, authentication, and trust services. In *Handbook of research on advancing cybersecurity for digital transformation.* Hershey, PA: IGI Global Scientific Publishing, 2021, pp. 18-36. https://doi.org/10.4018/978-1-7998-6975-7.ch002

[16] AFDHAL, Afdhal. Keabsahan identitas dalam administrasi kependudukan. *Jurnal Akta Yudisia,* 2018, vol. 3, no. 2, pp. 1-19. https://doi.org/10.35334/ay.v3i2.1549

examined five decisions of the Supreme Court and one of the Constitutional Court of Ukraine, addressing electronic signatures, digital documents, authentication tools, and electronic evidence. Examples include: Supreme Court (Case No. 120/4298/21-a, 07 Jul 2022) and Constitutional Court (Decision No. 4-r(II)/2021). All analysed rulings with full details and registry links are presented in Annex II (Judicial Decisions Analysed).

Case selection followed a documented search strategy using reyestr.court.gov.ua, HUDOC, and EUR-Lex, with queries such as "electronic signature," "digital identification," "BankID," and a cut-off date of January 2024. Only publicly accessible and legally reasoned cases concerning authentication or electronic evidence were included. Finally, the empirical base was complemented by a content analysis of open data from the MDT, NBU, Central Certification Authority, State Enterprise "Diia," and parliamentary committees to assess their institutional capacity for secure e-identification.

The third stage employed a comparative-legal approach to analyse legislation from Estonia, Poland, Germany, France, Lithuania, and the United States, focusing on identification models, assurance levels (eIDAS vs NIST), and the balance of public-private responsibility, identifying practices applicable to Ukraine's framework modernisation.

3.1. Research methods

The research employed dogmatic and theoretical-legal analysis of Ukrainian and foreign legislation (Poland, Lithuania, Estonia, Germany, France, and the United States), legal interpretation of digital identification norms, and comparative-legal and forecasting methods to evaluate future regulatory trends. It also included an empirical analysis of five judicial decisions – four of the Supreme Court and one of the Constitutional Court of Ukraine – addressing electronic signatures, digital evidence, and access to e-services. This was complemented by a content analysis of institutional practices of the Ministry of Digital Transformation, the National Bank, the Central Certification Authority, and the State Enterprise Diia.

3.2. Sampling

The research sample was formed according to the principles of relevance, official validity, and legal applicability. It included seven legislative and technical acts regulating electronic identification in Ukraine (listed in Annex I), and five judicial decisions – four of the Supreme Court and one of the Constitutional Court of Ukraine (Annex II).

Comparative material comprised legislation from six jurisdictions – Poland, Estonia, Germany, France, Lithuania, and the United States – representing both public PKI and private identity-provider models.

Additionally, official data from the Ministry of Digital Transformation, the National Bank, the Central Certification Authority, State Enterprise "Diia", and parliamentary committees were examined through content analysis to assess institutional capacity and regulatory effectiveness in digital identification.

3.3. Research tools

To support the empirical and comparative stages of the study, a range of legal, technical, and analytical instruments was employed to collect, verify, and interpret normative and case-law materials. The following tools were used:

– Legal and judicial databases: zakon.rada.gov.ua, reyestr.court.gov.ua, HUDOC, EUR-Lex.[17]

– National registers and technical documents for MobileID, BankID, and Diia.Signature systems.

– Analytical reports and recommendations from international organisations: ENISA, OECD, ITU.[18]

– Methodological documents and standards: eIDAS Regulation (EU No 910/2014), ETSI TS 119 431.[19]

The use of these sources ensured both the legal depth and practical reliability of the conclusions on the administrative and legal regulation of electronic identification in Ukraine.

---

[17] VERKHOVNA RADA OF UKRAINE. Legislation of Ukraine. n.d. Available from https://zakon.rada.gov.ua/laws; STATE JUDICIAL ADMINISTRATION OF UKRAINE. Unified State Register of Court Decisions. n.d. Available from https://reyestr.court.gov.ua/; EUROPEAN COURT OF HUMAN RIGHTS. HUDOC database. n.d. Available from: https://hudoc.echr.coe.int/ukr#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}; EUROPEAN UNION. EUR-Lex: Access to European Union law. n.d. Available from https://eur-lex.europa.eu/homepage.html

[18] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). Official website. n.d. Available from https://www.enisa.europa.eu/; ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). Official website. n.d. Available from https://www.oecd.org/en.html; INTERNATIONAL TELECOMMUNICATION UNION (ITU). Official website. n.d. Available from https://www.itu.int/fr/Pages/default.aspx#/fr

[19] EUROPEAN COMMISSION. eIDAS Regulation. n.d. Available from: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation; UKRAINIAN RESEARCH AND TRAINING CENTER FOR STANDARDIZATION, CERTIFICATION AND QUALITY (SE "UKRNDNC"). DSTS ETSI TS 119 431-1:2022 – Electronic Signatures and Infrastructures (ESI). Policy and security requirements for Trust Service Providers. Part 1: TSP service components operated with remote QSCD/SCDev. 2022. Available from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=98924

4. Results

The legislative framework for electronic identification in Ukraine remains fragmented and inconsistent, with conflicts between the Law of Ukraine "On Electronic Trust Services" and subordinate acts. The law regulates qualified electronic signatures but fails to define or recognise other authentication methods – notably BankID and MobileID – as legally valid means of identification in administrative or private transactions.

The Law of Ukraine "On Personal Data Protection" also lacks detailed procedures for protecting individuals during electronic identification, especially in cases of indirect data transfer through intermediary technical services, which generates legal uncertainty and weakens users' rights.

Ukraine's current regulation is not aligned with the EU eIDAS Regulation (2024/1183), which establishes standards for cross-border recognition, assurance levels (LoA), and security of digital identification. This regulatory gap hinders Ukraine's integration into the European digital space and prevents mutual recognition of electronic identities with EU Member States.Table 1 summarises the key regulatory acts and the conflicts identified between them.

Table 1. Conflicts in national legislation regarding electronic identification

Regulation/document	Key provisions	Conflict/problem
The Law of Ukraine "On Electronic Trust Services"	Regulates electronic signatures, but does not cover other means of identification (BankID, MobileID)	The authentication methods used do not have a fixed legal status.
The Law of Ukraine "On Protection of Personal Data"	Does not establish procedures for protecting individuals during identification in an electronic environment	Insufficient legal protection of personal data during identification.
Resolution of the Cabinet of Ministers of Ukraine No. 822 (dated 14 November 2018)	Introduces a single state web portal for administrative services without straightforward integration of all forms of identification	Lack of unified regulatory integration of digital services and means of identification
BankID/MobileID systems (actual practice)	Used in practice, but no precise legal regulation	Use of systems does not meet administrative procedure requirements
Regulation (EU) No. 2024/1183 (European Parliament & Council of the European Union, 2024)	Provides for mutual recognition of electronic identification in EU countries, absent in Ukrainian law	Inconsistency of Ukrainian legislation with European standards

Source: compiled by the author based on judicial decisions listed in Annex I (Legislative Acts Analysed)

An analysis of five Supreme Court rulings and one Constitutional Court decision revealed inconsistencies in interpreting the legal status of electronic signatures, authentication tools, and digital evidence. In *SCU, Case No. 120/4298/21-a (07 Jul*

2022), the court recognised an official electronic address as valid for service, emphasising the role of authentication over identification. Conversely, *SCU, Case No. 755/1549/22 (22 Mar 2023)* required verification of the electronic original, not a printed copy, while *Case No. 205/.

Table 2 systematises examples of contradictions in the interpretation of the legal status of electronic identification means in Ukrainian court practice, in particular about electronic signatures, digital evidence and technical means of authentication.

Table 2. Examples of contradictions in the interpretation of court decisions regarding electronic identification

Case number	The essence of the matter	Court position	Identified problem
120/4298/21-a	Official electronic address and proper service of court decisions.	Recognised the concept of an official electronic address but noted procedural ambiguity in its application.	Incomplete procedural regulation for the use of official electronic addresses and delivery of e-decisions.
755/1549/22	Verification of the electronic original rather than a paper copy.	Confirmed that courts must check the original digital document instead of relying on printed copies.	Unclear criteria for the verification of authenticity and validity of digital documents.
205/5252/19	Verification of pleadings emailed to the court when signed with a qualified e-signature (QES).	Established the duty of courts to verify authenticity of documents sent via e-mail with a qualified e-signature.	Lack of a unified verification protocol for documents submitted electronically.
4-r(II)/2021 (CCU)	The constitutionality of restricting access to social services through electronic registration.	Affirmed the principle of equal access but failed to define the legal status of digital identification.	Absence of a legal definition for digital identity as a separate category.
Grand Chamber, 03.08.2023	The admissibility of electronic correspondence as evidence.	Recognised electronic correspondence as admissible evidence if authorship and integrity are verified.	Lack of standardized procedures for verification and admission of electronic evidence.

Source: compiled by the author based on judicial decisions listed in Annex II (Judicial Decisions Analysed)

Judicial practice on electronic identification and authentication in Ukraine shows gradual stabilisation, particularly regarding the Qualified Electronic Signature (QES) and the admissibility of digital evidence. In *SCU, Case No. 120/4298/21-a (07 Jul 2022)*, the Court recognised an official electronic address as a valid means of communication, confirming the legal effect of authentication. Conversely, in *Case No. 755/1549/22 (22 Mar 2023)*, the Supreme Court ruled that only the verified electronic original constitutes valid evidence, while *Case No. 205/5252/19 (03 May 2022)* reaffirmed the duty of courts to check the authenticity of pleadings signed with QES.

The *Grand Chamber decision of 03 Aug 2023* marked a shift by recognising electronic correspondence as admissible evidence, provided that authorship and integrity can be verified. Meanwhile, the *Constitutional Court's Decision No. 4-r(II)/2021* confirmed equality of access to e-services but left the legal status of digital identity undefined. To ensure consistent interpretation, it is recommended to adopt a unified judicial guideline defining identification, authentication, and authorisation criteria under national law, harmonised with eIDAS 2.0 and technical standards such as ISO/IEC 24760-1:2019 and NIST SP 800-63 Rev.4. Establishing a verification protocol for QES and remote authentication would align Ukrainian practice with EU assurance levels and reduce evidentiary uncertainty.

Table 3 summarises typical approaches of courts to electronic authentication, in particular the conditions for accepting QES, the admissibility of authorisation via BankID/MobileID, and the underdevelopment of mechanisms for technical verification of a person's actions.

Table 3. Common court positions on electronic authentication (QES)

Judicial Position	Representative Case	Legal Issue / Problem
Recognition of an official electronic address as a valid channel for communication and authentication.	SCU, Case No. 120/4298/21-a (07 Jul 2022)	Procedural ambiguity in using official e-addresses for serving decisions.
Verification of the electronic original instead of printed copies.	SCU, Case No. 755/1549/22 (22 Mar 2023)	Lack of clear criteria for authenticity and validity of digital documents.
Mandatory verification of pleadings signed with QES sent via e-mail.	SCU, Case No. 205/5252/19 (03 May 2022)	Absence of a unified verification protocol for electronically filed documents.
Admissibility of electronic correspondence as evidence if integrity and authorship are proven.	Grand Chamber SCU (03 Aug 2023)	No standard procedure for verifying electronic evidence.
Constitutional protection of equality in access to e-services, without defining digital identity.	CCU, Decision No. 4-r(II)/2021 (16 Feb 2021)	No legal definition of "digital identity" or assurance levels.

Source: compiled by the author based on judicial decisions listed in Annex II (Judicial Decisions Analysed)

A comparative analysis of electronic identification models in Poland, Estonia, Germany, France, the United States, and Lithuania reveals diverse organisational and technical approaches. In Poland and Lithuania, a centralised PKI-based model linked to national ID cards operates in full compliance with eIDAS assurance levels. Estonia, by contrast, combines PKI-based e-identification for citizens with KSI blockchain technology used exclusively to ensure the integrity of state records, not for user

authentication. Germany and France apply multi-modal systems that integrate ID cards, mobile authentication, and biometric credentials governed by technical standards (ETSI TS 119 431, ISO/IEC 24760-1).

The United States follows a decentralised, multi-provider ecosystem guided by the NIST SP 800-63 Rev. 4 framework, which defines IAL, AAL, and FAL assurance levels instead of a single national eID law. Overall, public PKI-based models (Estonia, Poland) demonstrate higher trust and accountability but require strong central oversight, whereas private or hybrid models (United States, France) provide flexibility at the cost of legal fragmentation. European jurisdictions are converging through eIDAS 2.0, while Ukraine has yet to align its national framework with cross-border identification standards.

Table 4 provides a comparative overview of the legal regulation models for electronic identification in selected countries, focusing on the type of identification, legal basis and technical features.

Table 4. Key characteristics of legal regulation of electronic identification in selected countries

Country	Identification model	Legal basis	Features
Estonia	State PKI + e-Residency; KSI blockchain used only for integrity of state records	Electronic Identification and Trust Services for Electronic Transactions Act (Estonia, 2016, consolidated)	Advanced PKI-based identity; blockchain ensures integrity, not authentication
Poland	Centralised PKI via national ID card and Profil Zaufany	Platforma ePUAP and Profil Zaufany legal framework (Poland)	Broad population coverage; strong state control and interoperability
Lithuania	State PKI compatible with EU trust framework	Law on Electronic Identification and Trust Services for Electronic Transactions (Act No. XIII-1120, Lithuania, 2018)	Simplified, EU-aligned model; high cross-border compatibility
Germany	Multi-identification: ID card, mobile authentication, biometrics	Personalausweisgesetz / PAuswG (Germany, consolidated 2024)	Emphasis on technical security, interoperability, and user choice
France	Multi-identification with national ID and biometric options	Code de la sécurité intérieure (France, consolidated 2024)	Comprehensive regulation; integrates privacy and multi-channel authentication
United States	Decentralised multi-provider ecosystem (private IdPs, credit bureaus, DMVs)	NIST SP 800-63-4: Digital Identity Guidelines (United States, 2025)	Flexible, decentralised system; no single federal eID; relies on assurance levels (IAL/AAL/FAL)

Source: compiled by the author based on the legislative acts listed in Annex III (Legislative Acts of Selected Countries) and analytical materials from the eIDAS Regulation, ENISA, and NIST SP 800-63-4 guidelines.

A comparative analysis shows that the Ukrainian model is closest to the state PKI

systems of Poland and Lithuania, which already comply with eIDAS and can be integrated without major changes. The German multi-identification model is technically viable but needs legal clarification on biometric use. The Estonian blockchain-based e-Residency requires major institutional reform, while the decentralised U.S. system under NIST SP 800-63 is not compatible with Ukraine's legal environment. The main advantages include greater trust and interoperability with the EU system, whereas the key risks are legal fragmentation, limited technical readiness, and inter-agency coordination barriers. Table 5 systematises the assessment of the legal and technical implementation of leading foreign models in the context of Ukrainian legislation.

Table 5. Analysis of the implementation potential of foreign approaches

Country	Legal compatibility with Ukrainian law	Technical adaptability	Main risks
Estonia (e-Residency, blockchain)	Low – no legal analogue of blockchain-based identity	Limited – requires registry modernisation	Lack of legal framework and institutional support
Poland (PKI, Profil Zaufany)	High – PKI model aligned with Ukrainian system	High – infrastructure partially implemented	Need to strengthen personal-data safeguards
Germany (multi-ID, eID)	Medium – biometric use requires clear regulation	Medium – standardised protocols yet to be adopted	Risks linked to biometric data protection
France (standardised eID)	High – full eIDAS compatibility and clear norms	High – technically interoperable with Ukrainian platforms	Moderate financial costs for technical integration
United States (private IdP ecosystem, NIST SP 800-63)	Low – no unified federal law	Low – high decentralisation, no gateways	Insufficient state control, risk of commercialisation
Lithuania (eIDAS-compliant PKI)	High – fully compatible PKI structure	High – implementation feasible without major changes	Partial integration with domestic registers

Source: compiled by the author based on the legislative acts listed in Annex III.

The Ministry of Digital Transformation of Ukraine serves as the primary body responsible for electronic identification, mainly through the "Diia" ecosystem, yet its regulatory mandate remains limited. The National Bank of Ukraine operates the BankID system without direct legislative competence. The Central Certification Authority provides technical infrastructure but lacks effective coordination with other institutions. The State Enterprise "Diia" acts as a service operator without a formally defined legal status. Parliamentary committees introduce relevant legislative initiatives; however, the absence of a unified inter-agency strategy continues to slow institutional reform. Table 6 presents an assessment of the institutional effectiveness of the central state bodies involved in the regulation and implementation of electronic identification

in Ukraine.

Table 6. Assessment of institutional effectiveness in the field of electronic identification

Institution	Functions in the field of electronic identification	Effectiveness / regulatory assessment
Ministry of Digital Transformation of Ukraine (MDT)	Formulates state digital policy, develops e-identification infrastructure, coordinates implementation of "Diia" ecosystem	High administrative capacity; limited regulatory authority
National Bank of Ukraine (NBU)	Administers the BankID system, sets technical and procedural requirements for financial sector identification	Technically stable framework; absence of legislative competence beyond financial domain
Central Certification Authority (CCA)	Manages national cryptographic keys and ensures technical compliance with trust standards	Reliable technical base; insufficient coordination with other institutions
State Enterprise "Diia" (SE Diia)	Provides e-services and integrates identification mechanisms within public platforms	Effective operational integration; lacks defined legal personality in regulatory acts
Parliamentary Committees (Digital Transformation, Legal Policy)	Draft and review legislation in the area of e-identification and personal data protection	Active legislative initiative; absence of unified inter-agency coordination strategy

Source: compiled by the author based on institutional reports of the Ministry of Digital Transformation of Ukraine, the National Bank of Ukraine, and parliamentary records, as well as the legislative acts listed in Annex I (Legislative Acts Analysed).

The results confirm the need for targeted legislative and administrative amendments to strengthen Ukraine's national electronic identification framework. Harmonising the Law "On Electronic Trust Services" with the eIDAS Regulation, defining the legal status of BankID and MobileID, and introducing a unified procedure for QES verification would ensure legal consistency and interoperability. Aligning judicial practice with technical assurance standards (ISO/IEC 24760 and NIST SP 800-63-4) will enhance the reliability, transparency, and cross-border recognition of digital identification in interactions between citizens and public authorities.

5. Discussion

The results obtained confirm the fragmentary nature of regulatory control over electronic identification, technical vulnerability, and legal ambiguity of its application in public administration. This creates a basis for further clarification of the legal status of digital identity in administrative proceedings.

The position of Semenets-Orlova et al., which emphasises the need for developing the digital competence of administrators and for the formalisation of remote

interaction procedures, is partially consistent with the findings identified herein.[20] However, the study above is predominantly focused on the sphere of education. In contrast, the analysis of legal application in this research encompasses a broader spectrum of public law relations, specifically including administrative litigation and the legal status of electronic transactions.

A similar partial correspondence was also identified concerning the conclusions of Omelchuk et al., who investigate the use of electronic evidence in criminal procedure.[21] Despite the different procedural spheres, a common problem emerges: the absence of a clear legal definition for the status of digital documents. The analysis of administrative judicial practice herein also corroborates this finding.

A study by Sahatatua et al. on data leaks in Indonesia highlights the vulnerability of centralised systems without proper controls and accountability mechanisms.[22] This conclusion is consistent with the findings regarding legal uncertainty in the field of personal data protection in Ukraine's state electronic registers, which undermines trust in digital services.

Tucker analyses the use of facial recognition systems in border control, acknowledging their effectiveness but simultaneously emphasising the need for legal regulation.[23] This position partially aligns with the conclusions of our analysis, which also accentuates the risks associated with the unregulated collection and processing of biometric data in public law relations.

Müller-Torok and Bader link the limited spread of eIDAS-compliant identifiers to low trust levels and complexity of use.[24] This position correlates with the problems of information secrecy and the technical complexity of BankID and MobileID procedures

[20] SEMENETS-ORLOVA, Inna, et al. Special aspects of educational managers' administrative activity under conditions of distance learning. *Journal of Curriculum and Teaching*, 2022, vol. 11, no. 1, pp. 286-297. https://doi.org/10.5430/jct.v11n1p286

[21] OMELCHUK, Oleh M., et al. Analysis of the activities of law enforcement authorities in the field of combating crime and corruption offences. *Journal of Money Laundering Control*, 2022, vol. 25, no. 3, pp. 700-716. https://doi.org/10.1108/JMLC-07-2021-0073

[22] SAHATATUA, Richart, et al. Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a Hacker Forum. *Journal of Multidisciplinary Academic and Practice Studies*, 2024, vol. 2, no. 3, pp. 261–265. https://doi.org/10.35912/jomaps.v2i3.2219

[23] TUCKER, Aaron. The citizen question: Making Identities Visible Via Facial Recognition Software at the Border. *IEEE Technology and Society Magazine*, 2020, vol. 39, no. 4, pp. 52-59. https://doi.org/10.1109/MTS.2020.3031847

[24] MÜLLER-TOROK, Robert and BADER, Lea. Identification issues in citizens' participation. Why are eIDAS-compliant means of identification not a common standard? In *CEEeGov '22: Proceedings of the Central and Eastern European eDem and eGov Days.* New York, United States: Association for Computing Machinery, 2022, pp. 118-122. https://doi.org/10.1145/3551504.3552325

identified in Ukraine. The thesis about the need not only for regulation but also for improving the functional convenience of digital services is supported.

Sharma, analysing the case of Assam in India, demonstrates the risks of legally excluding individuals from the public sphere due to a lack of digital identification.[25] Similar risks are partially confirmed in the Ukrainian context, where limited digital access can hinder the realisation of administrative rights, especially for vulnerable groups. This highlights the need for legal safeguards against the discriminatory effects of digital authentication.

Dërmaku and Raif Emini point to an imbalance between the pace of digitalisation and regulatory reform in Kosovo, which undermines the stability of public services.[26] A similar trend can be observed in Ukraine: digital solutions are being implemented dynamically, but the legal framework is not keeping pace with technical changes, resulting in fragmented law enforcement.

Tianyu and Ruijia draw attention to the weak regulatory control over the processing of personal data within the framework of big data in China, which blurs the line between administrative functions and technical processes.[27] This problem is also relevant for Ukraine, where the regulatory framework for digital privacy remains fragmented, despite the active introduction of electronic identification.

Bradul et al. analyse the electronic taxpayer account as an example of fiscal digitalisation, emphasising its potential for administrative transparency.[28] However, the results of the study confirm that in the absence of clear standards for the protection of digital identification, such services do not provide an adequate level of trust and efficiency.

Madsen et al. explore the phenomenon of the “accidental bureaucrat”, where digital services delegate administrative functions to citizens.[29] This observation is

[25] SHARMA, Chetna. Documents for identity: Citizenship impasse in Assam, India. Ethnicities, 2021, vol. 23, no. 2, pp. 192-212. https://doi.org/10.1177/14687968211046965

[26] DËRMAKU, Kastriot and RAIF EMINI, Ardian. Digitisation of Administration and Legal Basis in Kosovo. *Access to Justice in Eastern Europe*, 2024, vol. 1, no. 22. https://doi.org/10.33327/ajee-18-7.1-a000107

[27] TIANYU, Ju and RUIJIA, Wu. Research on administrative law protection of personal information under the background of big data. *Academic Journal of Humanities & Social Sciences,* 2021, vol. 4, no. 7, pp. 90-92. https://doi.org/10.25236/AJHSS.2021.040717

[28] BRADUL, Alexander, ADAMOVSKA, Victoria and SHEPELIUK, Vira. Prospects for implementing the taxpayer's e-cabine. *Scientific Notes of the University KROK,* 2020, vol. 3, no. 56, pp. 46-51. https://doi.org/10.31732/2663-2209-2020-59-46-51

[29] MADSEN, Christian, LINDGREN, Ida, MELIN, Ulf. The accidental caseworker – How digital self-service influences citizens' administrative burden. *Government Information Quarterly,* 2021, vol. 39, no. 1. https://doi.org/10.1016/j.giq.2021.101653

relevant to Ukraine, where electronic identification often complicates access to services, turning into a barrier instead of a facilitator. Such a situation calls for a rethinking of the functional design of digital tools.

Guštin emphasises the need for a differentiated approach to electronic identification, taking into account the age and legal characteristics of subjects, especially children.[30] The universalisation of technical solutions without considering the social context creates risks of discrimination and limits access to administrative procedures for vulnerable groups.

Przemysław emphasises the importance of the principle of *in dubio pro libertate* as a tool for limiting excessive state interference in administrative matters.[31] In the field of digital identification, this principle could guarantee access to services even in the absence of electronic authentication. However, its weak implementation in Ukrainian law reduces its practical effectiveness, as confirmed by an analysis of judicial practice.

Maculuve and Amaral note that the effectiveness of digital identification systems depends on the level of legal culture, technological access, and trust in the state.[32] A similar imbalance has been identified in Ukraine, where technical implementation is ahead of regulatory support, limiting the effectiveness of digital transformation.

Shvaika emphasises the role of the Security Service of Ukraine in shaping the system of state control over digital data flows, including electronic identification.[33] This position is consistent with our research findings on the need for inter-agency coordination and the institutionalisation of control over digital authentication processes.

Panjaitan emphasises that even automated administrative decisions must comply with the principles of fairness, be accessible for review and undergo institutional oversight.[34] An analysis of judicial practice in Ukraine confirms the risks of the absence

[30] GUŠTIN, Matko. Protection of procedural rights of the child in administrative proceedings with special reference to proceedings related to status law issues. *Child and Family in Contemporary Society,* 2021, vol. 1, no. 1, pp. 27–62. https://doi.org/10.25234/dosd/31050

[31] PRZEMYSŁAW, Sztejna. The principle of in dubio pro libertate in administrative proceedings and its function: A step forward or a step back? *Krytyka Prawa*, 2021, vol. 12, no. 4, pp. 161-177. https://doi.org/10.7206/KP.2080-1084.415

[32] MACULUVE, Paulo and AMARAL, Luis. Reflection on African citizen identification systems. *CAPSI 2023 Proceedings,* 2023, 6. https://doi.org/10.18803/capsi.v23.01-17

[33] SHVAIKA, Mykola. The place and importance of the Security Service of Ukraine in the implementation of the administrative and legal mechanism for ensuring the rights and freedoms of citizens. *Analytical and Comparative Jurisprudence*, 2023, no. 4, pp. 282-286. https://doi.org/10.24144/2788-6018.2023.04.47

[34] PANJAITAN, Marojahan. The legal impacts and the government's efforts to respond to electronic state administrative decisions following the enactment of law no. 11 of 2020 on job creation. *Prophetic Law Review*, 2022, vol. 4, no. 1, pp. 110-130. https://doi.org/10.20885/plr.vol4.iss1.art6

of appeal mechanisms in the case of electronic actions, which indicates the need for regulatory refinement of digital procedures.

Thus, the results of the analytical comparison confirm the need for a cautious and structured approach to the introduction of electronic identification in public administration. Technical functionality without adequate legal support cannot guarantee the observance of citizens' rights and freedoms. Current practice indicates that only under conditions of legal predictability, transparency, and supervisory accountability can digital identity be integrated into the public law system without threatening public legitimacy and social trust.

5.1. Limitations

The study is limited by the geographical and regulatory context of Ukraine, which complicates the complete application of its conclusions to other legal systems. In addition, the insufficient availability of official technical specifications for state identification platforms limited the depth of the technical and legal analysis.

5.2. Recommendations

To enhance the coherence and reliability of Ukraine's electronic identification framework, it is recommended to:

- amend the Law "On Electronic Trust Services" to define the legal status of BankID and MobileID as recognised means of identification in administrative procedures;
- adopt a by-law establishing a unified procedure for the verification and evidentiary use of Qualified Electronic Signatures (QES);
- introduce technical standards for audit trails, time-stamping, and data integrity consistent with ISO/IEC 24760 and NIST SP 800-63-4; and
- align Ukrainian assurance levels with those set by the eIDAS Regulation to ensure cross-border interoperability and legal equivalence.

6. Conclusions

The study confirms the fragmented and inconsistent nature of administrative and legal regulation of electronic identification in Ukraine. The absence of a unified definition of authentication methods and the unclear legal status of BankID and MobileID hinder the effective application of electronic identification in administrative procedures. National standards remain unaligned with the eIDAS Regulation, ISO/IEC 24760, and NIST SP 800-63-4, which limits international interoperability.

Judicial analysis demonstrated divergence in the interpretation of electronic signatures and the admissibility of digital evidence, underscoring the need for a unified procedural framework. Institutional assessment revealed an imbalance between strong technical capacity and weak regulatory coordination among the Ministry of Digital Transformation, the National Bank of Ukraine, and the Central Certification Authority. A comparative legal review identified the models of Poland, Lithuania, and Germany as the most adaptable to Ukraine's context, enabling phased integration into the European trust ecosystem.

The research provides a normative basis for refining Ukraine's Law "On Electronic Trust Services," establishing a uniform QES verification procedure, and mapping national assurance levels to eIDAS standards. Its practical significance lies in offering draftable legal mechanisms to ensure the consistency, transparency, and cross-border recognition of electronic identification in Ukraine.

REFERENCES

AFDHAL, Afdhal. Keabsahan identitas dalam administrasi kependudukan. *Jurnal Akta Yudisia,* 2018, vol. 3, no. 2, pp. 1-19. https://doi.org/10.35334/ay.v3i2.1549

ALONSO, Álvaro, et al. Enhancing university services by extending the eIDAS European specification with academic attributes. *Sustainability*, 2020, vol. 12, no. 3, 770. https://doi.org/10.3390/su12030770

AMORIM, Joni A., DE SIQUERIA ROCHA, Jose and MAGAL-ROYO, Teresa. Cybersecurity in Europe: Digital identification, authentication, and trust services. In *Handbook of research on advancing cybersecurity for digital transformation.* Hershey, PA: IGI Global Scientific Publishing, 2021, pp. 18-36. https://doi.org/10.4018/978-1-7998-6975-7.ch002

BRADUL, Alexander, ADAMOVSKA, Victoria and SHEPELIUK, Vira. Prospects for implementing the taxpayer's e-cabine. *Scientific Notes of the University KROK,* 2020, vol. 3, no. 56, pp. 46-51. https://doi.org/10.31732/2663-2209-2020-59-46-51

CHIANG, Daud and HOESIN, Zainal. Ensuring equality before the law and personal data protection through implementation of AI integration in single identification number systems: A positivist philosophy perspective. *Devotion - Journal of Research and Community Service,* 2024, vol. 5, no. 11, pp. 1347-1361. https://doi.org/10.59188/devotion.v5i11.20688

CORREA-MARICHAL, Javier, et al. Study and security analysis of the Spanish identity card. *Cryptography and Security,* 2022. https://doi.org/10.48550/arXiv.2210.04064

DAGIRAL, Eric and SINGH, Khertimayum. Governance and accountable citizenship through identification infrastructures: Database politics of Copernicus (France) and National Register of Citizens (India). *Science, Technology and Society*, 2020, vol. 25, no. 3, pp. 368-385. https://doi.org/10.1177/0971721820912895

DËRMAKU, Kastriot and RAIF EMINI, Ardian. Digitisation of Administration and Legal Basis in Kosovo. *Access to Justice in Eastern Europe*, 2024, vol. 1, no. 22. https://doi.org/10.33327/ajee-18-7.1-a000107

DIIA. Official website. n.d. https://se.diia.gov.ua/

EUROPEAN COURT OF HUMAN RIGHTS. HUDOC database. n.d. Available from: https://hudoc.echr.coe.int/ukr#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}

EUROPEAN UNION. EUR-Lex: Access to European Union law. n.d. Available from https://eur-lex.europa.eu/homepage.html

GOLIĆ, Darko. Normative regulation of electronic administration in the Republic of Serbia. *Pravo - Teorija i Praksa*, 2023, vol. 40, pp. 44-62. https://doi.org/10.5937/ptp2300044g

GUŠTIN, Matko. Protection of procedural rights of the child in administrative proceedings with special

reference to proceedings related to status law issues. *Child and Family in Contemporary Society,* 2021, vol. 1, no. 1, pp. 27–62. https://doi.org/10.25234/dosd/31050

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) & INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). ISO/IEC 24760-1:2019 – Information security, cybersecurity and privacy protection – A framework for identity management – Part 2: Reference architecture and requirements. 2019. Available from https://www.iso.org/ru/standard/81953.html

INTERNATIONAL TELECOMMUNICATION UNION (ITU). Official website. n.d. Available from https://www.itu.int/fr/Pages/default.aspx#/fr

MACAN, Siniša. Legal acceptability of the security level of the electronic identification system. *Godišnjak Fakulteta Pravnih Nauka,* 2021, vol. 11, no. 11, pp. 186-199. https://doi.org/10.7251/gfp2111186m

MACULUVE, Paulo and AMARAL, Luis. Reflection on African citizen identification systems. *CAPSI 2023 Proceedings,* 2023, 6. https://doi.org/10.18803/capsi.v23.01-17

MADSEN, Christian, LINDGREN, Ida, MELIN, Ulf. The accidental caseworker – How digital self-service influences citizens' administrative burden. *Government Information Quarterly,* 2021, vol. 39, no. 1. https://doi.org/10.1016/j.giq.2021.101653

MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE. Official website. n.d. Available from: https://thedigital.gov.ua/

MÜLLER-TOROK, Robert and BADER, Lea. Identification issues in citizens' participation. Why are eIDAS-compliant means of identification not a common standard? In *CEEeGov '22: Proceedings of the Central and Eastern European eDem and eGov Days.* New York, United States: Association for Computing Machinery, 2022, pp. 118-122. https://doi.org/10.1145/3551504.3552325

NATIONAL BANK OF UKRAINE. Official website. n.d. Available from: https://bank.gov.ua/

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Digital identity guidelines (NIST Special Publication 800-63-3). 2024. Available from https://pages.nist.gov/800-63-3/

OMELCHUK, Oleh M., et al. Analysis of the activities of law enforcement authorities in the field of combating crime and corruption offences. *Journal of Money Laundering Control*, 2022, vol. 25, no. 3, pp. 700-716. https://doi.org/10.1108/JMLC-07-2021-0073

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). Official website. n.d. Available from https://www.oecd.org/en.html

PÁEZ, Rafael, et al. An architecture for biometric electronic identification document system based on blockchain. *Future Internet*, 2020, vol. 12, no. 1, 10. https://doi.org/10.3390/fi12010010

PANJAITAN, Marojahan. The legal impacts and the government's efforts to respond to electronic state administrative decisions following the enactment of law no. 11 of 2020 on job creation. *Prophetic Law Review*, 2022, vol. 4, no. 1, pp. 110-130. https://doi.org/10.20885/plr.vol4.iss1.art6

PRZEMYSŁAW, Sztejna. The principle of in dubio pro libertate in administrative proceedings and its function: A step forward or a step back? *Krytyka Prawa*, 2021, vol. 12, no. 4, pp. 161-177. https://doi.org/10.7206/KP.2080-1084.415

SAHATATUA, Richart, et al. Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a Hacker Forum. *Journal of Multidisciplinary Academic and Practice Studies*, 2024, vol. 2, no. 3, pp. 261–265. https://doi.org/10.35912/jomaps.v2i3.2219

SEMENETS-ORLOVA, Inna, et al. Special aspects of educational managers' administrative activity under conditions of distance learning. *Journal of Curriculum and Teaching*, 2022, vol. 11, no. 1, pp. 286-297. https://doi.org/10.5430/jct.v11n1p286

SHARMA, Chetna. Documents for identity: Citizenship impasse in Assam, India. Ethnicities, 2021, vol. 23, no. 2, pp. 192-212. https://doi.org/10.1177/14687968211046965

SHVAIKA, Mykola. The place and importance of the Security Service of Ukraine in the implementation of the administrative and legal mechanism for ensuring the rights and freedoms of citizens. *Analytical and Comparative Jurisprudence*, 2023, no. 4, pp. 282-286. https://doi.org/10.24144/2788-6018.2023.04.47

STATE JUDICIAL ADMINISTRATION OF UKRAINE. Unified State Register of Court Decisions. n.d. Available from https://reyestr.court.gov.ua/

SUBRAMANIAN, Vidya. Citizenship in India: Parsing the complexity of digital identity systems. *Science, Technology and Society*, 2024, vol. 29, no. 4, pp. 595-613. https://doi.org/10.1177/09717218241281940

SUDIARAWAN, Kadek, et al. Discourses on citizen lawsuit as administrative dispute object: Government administration law vs. administrative court law. *Journal of Indonesian Legal Studies,* 2022, vol. 7, no. 2, pp. 499-486. https://doi.org/10.15294/jils.v7i2.60166

TIANYU, Ju and RUIJIA, Wu. Research on administrative law protection of personal information under the background of big data. *Academic Journal of Humanities & Social Sciences,* 2021, vol. 4, no. 7, pp. 90-92. https://doi.org/10.25236/AJHSS.2021.040717

TUCKER, Aaron. The citizen question: Making Identities Visible Via Facial Recognition Software at the Border. *IEEE Technology and Society Magazine*, 2020, vol. 39, no. 4, pp. 52-59. https://doi.org/10.1109/MTS.2020.3031847

UKRAINIAN RESEARCH AND TRAINING CENTER FOR STANDARDIZATION, CERTIFICATION AND QUALITY (SE "UKRNDNC"). DSTS ETSI TS 119 431-1:2022 – Electronic Signatures and Infrastructures (ESI). Policy and security requirements for Trust Service Providers. Part 1: TSP service components operated with remote QSCD/SCDev. 2022. Available from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=98924

UNIFIED STATE WEBPORTAL OF ELECTRONIC SERVICES DIIA. n.d. Available from: https://se.diia.gov.ua/unified-state-web-portal-of-electronic-services-diia

Annex I. Legislative Acts Analysed

No.	Title of the Act / Document	Jurisdiction	Reference Number / Year	Last Amendment	Source (Official Link)
1	Law of Ukraine 'On Electronic Trust Services'	Ukraine	No. 2155-VIII (2017)	as of 2023	https://zakon.rada.gov.ua/laws/show/2155-19
2	Law of Ukraine 'On Personal Data Protection'	Ukraine	No. 2297-VI (2010)	as of 2023	https://zakon.rada.gov.ua/laws/show/2297-17
3	Resolutions of the Cabinet of Ministers of Ukraine (CMU)	Ukraine	–	–	https://zakon.rada.gov.ua/laws
4	Regulations of the National Bank of Ukraine (NBU) and the Ministry of Digital Transformation (MDT)	Ukraine	–	–	https://bank.gov.ua/ ; https://thedigital.gov.ua/
5	Regulation (EU) 2024/1183 (eIDAS 2.0)	European Union	Regulation (EU) 2024/1183	–	https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
6	ISO/IEC 24760-1:2019 + Amd 1:2023 'IT Security and Privacy – Identity Management'	International	ISO/IEC 24760-1 (2019, Amd 2023)	2023	https://www.iso.org/standard/77582.html
7	NIST SP 800-63 Rev. 4 (2024) 'Digital Identity Guidelines'	United States	NIST SP 800-63 Rev.4 (2024)	2024	https://pages.nist.gov/800-63-4/

Annex II. Judicial Decisions Analysed

No.	Court	Case No.	Date	Official Source (Primary)	URL	Legal Issue
1	Supreme Court of Ukraine (Administrative Cassation Court)	120/4298/21-a	07 July 2022	JurLiga Legal Information Portal	https://jurliga.ligazakon.net/news/213934_verkhovniy-sud-rozyasniv-shcho--oftsynoyu-elektronnoyu-adresoyu	Official electronic address and proper service of court decisions.
2	Supreme Court of Ukraine (Civil Cassation Court)	755/1549/22	22 March 2023	JurLiga Legal Information Portal	https://jurliga.ligazakon.net/news/218999_sud-ma-perevryati-orignal-podanogo-v-elektronny-form-dokumenta-a-ne-yogo-paperovu-kopyu-vs	Verification of the electronic original rather than a paper copy.
3	Supreme Court of Ukraine (Civil Cassation Court)	205/5252/19	03 May 2022	JurLiga Legal Information Portal	https://jurliga.ligazakon.net/news/211407_ktss-vs-rozyasniv-shcho-cudi-zobovyazan-perevryati-protsesualn-dokumenti-podan-na-elektronnu-adresu-sudu-z-pdpisannyam-etsp	Verification of pleadings emailed to the court when signed with a qualified e-signature (QES).
4	Supreme Court of Ukraine (Grand Chamber)	Grand Chamber, 03.08.2023	03 August 2023	Supreme Court Press Centre	https://supreme.court.gov.ua/supreme/pres-centr/news/1458816/	Admissibility of electronic correspondence as evidence.
5	Constitutional Court of Ukraine	4-r(II)/2021	16 February 2021	Constitutional Court of Ukraine	https://ccu.gov.ua/dokument/4-rii2021	Constitutionality of restricting access to social services through electronic registration.

Annex III. Foreign Legislative and Standard Sources Analysed

Country	Official Source / Publisher	Act / Document	Date / Version	Official URL
Estonia	Riigi Teataja (State Gazette)	Electronic Identification and Trust Services for Electronic Transactions Act (consolidated version)	12 Oct 2016 (latest consolidation 2023–2025)	https://www.riigiteataja.ee/en/eli/527102016001/consolide
Poland	Republic of Poland – ePUAP Portal	Platforma ePUAP (Electronic Platform of Public Administration Services)	Ongoing official portal	https://www.epuap.gov.pl
Lithuania	Seimas (Lithuanian Parliament)	Law on Electronic Identification and Trust Services for Electronic Transactions (Act No. XIII-1120)	26 Apr 2018	https://e-seimas.lrs.lt/portal/legalAct/en/TAD/c5174772ecd011e89d4ad92e8434e309
Germany	Gesetze im Internet (Federal Ministry of Justice)	Act on Identity Cards and Electronic Identification (Personalausweisgesetz / PAuswG)	Latest consolidation 2024	https://www.gesetze-im-internet.de/englisch_pauswg/englisch_pauswg.html
France	Légifrance (French Government)	Code de la sécurité intérieure – sections on e-identification and security	Consolidated code 2024	https://www.legifrance.gouv.fr
United States	National Institute of Standards and Technology (NIST)	NIST Special Publication 800-63-4: Digital Identity Guidelines (IAL/AAL/FAL)	2025	https://pages.nist.gov/800-63-4/

Data de submissão do artigo: 10/08/2025

Data de aprovação do artigo: 17/10/2025

Edição e propriedade:
Universidade Portucalense Cooperativa de Ensino Superior, CRL
Rua Dr. António Bernardino de Almeida, 541 - 4200-072 Porto
Email: upt@upt.pt