Society. Document. Communication

Journal homepage: https://sdc-journal.com.ua/en
Society. Document. Communication, Vol. 11, No. 2, 47-57

Article's History: Received: 03.01.2026 Revised: 14.04.2026 Accepted: 12.05.2026 Published: 30.05.2026

UDC 004.738.5:34
DOI: 10.69587/sdc/2.2026.47

ISSN 2518-7600
e-ISSN 2524-1060

Regulatory and legal frameworks and standardisation of mechanisms for ensuring the authenticity of electronic documents in the age of generative content

Oksana Vasylynyna*
Lecturer
National University "Yuri Kondratyuk Poltava Polytechnic"
36011, 24 V. Hrytsaienko Ave., Poltava, Ukraine
https://orcid.org/0000-0003-0402-4627

Olha Mizina
PhD in Philological Sciences, Associate Professor
National University "Yuri Kondratyuk Poltava Polytechnic"
36011, 24 V. Hrytsaienko Ave., Poltava, Ukraine
https://orcid.org/0000-0002-1988-6353

Yaroslav Blokha
PhD in Philosophical Sciences, Associate Professor
National University "Yuri Kondratyuk Poltava Polytechnic"
36011, 24 V. Hrytsaienko Ave., Poltava, Ukraine
https://orcid.org/0000-0002-0799-1789

Abstract. The relevance of the study is conditioned by the growing risks of falsification of digital documents, forgery of electronic signatures, metadata manipulation, and distribution of synthetic content that replaces the content of authentic sources. The purpose of the study was to determine the theoretical foundations for the establishment of a comprehensive system for the protection of electronic documents, combining regulatory, technical, and information and analytical verification mechanisms, in the context of increasing risks of potentially destabilising impacts of artificial intelligence systems. The paper considered the regulatory framework, approaches, and mechanisms for ensuring the authenticity of electronic documents in the context of rapid development of content generated using artificial intelligence systems. The current Ukrainian legislation governing electronic trust services and document management was analysed, including the international standards of eIDAS, ETSI, ISO/IEC, and C2PA, which regulate issues relating to the authentication, integrity, and origin of electronic data. The features of advanced authentication technologies, in particular, qualified electronic signature, electronic seal, blockchain, digital watermarks, cryptographic hashes, and mechanisms for fixing the origin of content, were clarified. The specifics of the influence of generative content on the creation of fake documents, synthetic media, and disinformation campaigns were determined. The paper described the features of information analytics as an effective tool for identifying, evaluating, and minimising risks that are directly related to the use of generative content in electronic documents. It was proved that information and analytical methods allow for multi-level audit of data origin, metadata analysis, identification of signs of automated generation, and forecasting of threats to digital trust systems. It was proposed to consider information analytics as an integrative component of the contemporary electronic document authentication architecture, combining legal, technical, and organisational

Suggested Citation:
Vasylynyna, O., Mizina, O., & Blokha, Ya. (2026). Regulatory and legal frameworks and standardisation of mechanisms for ensuring the authenticity of electronic documents in the age of generative content. *Society. Document. Communication*, 11(2), 47-57. doi: 10.69587/sdc/2.2026.47.

*Corresponding author (o.vasylynyna@gmail.com)

mechanisms for ensuring information protection in the context of digital changes. The practical significance of the study lies in the possibility of using the results to implement a comprehensive approach to data authentication in electronic document management systems. In addition, the proposed approaches to analysing the origin of content, metadata, and features of generative processing allow creating systems for monitoring and auditing electronic documents to detect falsifications, synthetic materials, and manipulative content

Keywords: information protection; qualified electronic signature; metadata; artificial intelligence systems; standardisation; information analytics

Introduction

Intensive integration of artificial intelligence technologies in all spheres of public activity determines the need not only for technical control over their work, but also for a high-quality information and analytical assessment of the processes of creating, using, and distributing generative content in electronic documents. In this context, information analytics becomes a key tool for the development of a comprehensive data audit: it provides collection, verification, classification, and interpretation of information about data sources, algorithmic features of generated materials, their compliance with regulatory requirements, and potential risks. In the absence of reliable confirmation of sources, there is a risk that artificial intelligence systems will use biased, false, or copyrighted data without the appropriate consent of the copyright holders, which undermines the integrity and reliability of such systems. As indicated by S. Longpre *et al.* (2024), current practices include extensive use of sources and grouping of data without tracking or verifying their original sources, author's intentions, copyright and licensing status, or basic composition and properties.

M.R. Shoaib *et al.* (2023) pointed out in their paper that advanced artificial intelligence significantly increases the realism of artificially created and forged materials. This leads to a rapid increase in the volume of disinformation, cyber harassment, falsification of digital documents, and large-scale manipulation of public consciousness. Among innovative yet risky technologies, special attention is drawn to generative models, sophisticated machine learning algorithms, and large data processing models that can produce content that is difficult to distinguish from authentic sources. In these circumstances, information analytics becomes critical, because it provides a comprehensive approach to identifying, assessing and minimising the risks associated with the use of AI. Analytical methods allow performing multi-level verification of data reliability, identifying signs of automated generation and manipulative influences, modelling potential threats, and systematically analysing information flows in which fake or modified content is distributed.

The review of contemporary academic research, both in Ukraine and in the international sphere, shows the gradually increasing attention to the issues of authentication of electronic documents, in particular under the influence of artificial intelligence, and the associated risks to authenticity, trust, and information security. The paper by I. Khomych *et al.* (2025) focused on identifying the features of automated digital content creation to provide a comprehensive assessment of the authenticity of electronic documents during the rapid spread of AI technologies. The researchers emphasise that conventional approaches to recording digital signatures and metadata are not sufficient to counteract the risks of falsification and manipulation of digital data generated by artificial intelligence models. J. Sharma *et al.* (2026) examined new technical approaches for verifying the origin and authenticity of content, in particular, blockchain-based methods and vector similarity for separating AI-generated images from human works, which opens up prospects for digital authentication of multimedia documents. The paper by O. Ege *et al.* (2025) was devoted to the investigation of user aspects and the experience of using electronic signatures, which affects the perception of security and the availability of authentication on the part of end users. The paper highlighted the relationship between security, convenience, and trust in electronic authentication mechanisms.

Contemporary research focuses not only on the technical aspects of electronic data protection, but also on the issues of legal regulation of mechanisms for detecting generative content considering the analysis of metadata, the history of document creation and distribution. The developments of S.V. Hubariev & O.O. Loviak (2022) and A.L. Sviatoshniuk (2023) systematised the legal aspects of the use of electronic signatures, electronic documents, and trust services, identified gaps in current legislation, and interpreted regulatory requirements for the protection of digital authenticity. In these papers, the researchers emphasised the imperfection of legal regulation and the need to adapt Ukrainian norms to international standards in the field of electronic identification and digital trust. Despite this, the issue of integrating information and analytical approaches into the system of legal regulation of the authenticity of electronic documents, and evaluating their effectiveness in countering falsification and manipulation of digital data, remains rather neglected.

The purpose of the study was to investigate the state of regulatory regulation and standardisation of electronic document authentication mechanisms in Ukraine, compare it with international approaches and determine the areas of development in the context of generative

content distribution, and to substantiate the role of information analytics as a key tool for evaluating the effectiveness of these mechanisms. To achieve this goal, the following tasks were defined: to carry out a comparative analysis and to identify the main gaps in the current regulatory framework of Ukraine and international standards for the authentication of electronic documents in the context of the spread of generative technologies; to characterise emerging technologies for ensuring the authenticity of electronic documents; to determine the role and potential of information and analytical tools for detecting fake materials and predicting the risks of their distribution in the digital environment. The scientific originality of the study consists in a comprehensive overview of the characteristics of the current system of regulatory, legal, and technical safeguards for the authenticity of electronic documents, and in the identification of approaches to analysing the origin of content, metadata, and indicators of generative processing.

Materials and Methods

The study used an interdisciplinary approach that combines methods of comparative analysis of laws and regulations, system analysis, content analysis of sources, and scientific generalisation. This methodological combination was conditioned by the complex nature of the problem of ensuring the authenticity of data of electronic documents during the period of increasing risks of exposure to the content of artificial intelligence systems, which requires simultaneous consideration of legal, technical, and information and analytical dimensions. Comparative analysis of laws and regulations was used to compare the national model of electronic authentication regulation in Ukraine with European approaches. The objects of comparison were Ukraine and the European Union as legal systems with varying degrees of integration of digital trust mechanisms and AI regulation. Within the Ukrainian legal framework, the provisions of Law of Ukraine No. 2155-VIII (2017) have been analysed, specifically Article 1 (definition of authentication), Article 18 (legal consequences of the use of a qualified electronic signature), and Article 23 (requirements for trust services). Article 5-7 of the Law of Ukraine No. 851-IV (2003), which provide a legislative justification for the legal force of an electronic document and the conditions for its use as evidence. At EU level, articles 25 and 26 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council (2014) have been analysed; these articles set out the principles of the legal equivalence of electronic signatures. The comparison revealed regulatory gaps in regulating the origin and authenticity of AI-generated materials.

The system analysis method was used to structure the digital trust architecture as an integrated model that includes legal mechanisms, technical standards, and information and analytical audit and monitoring tools. This approach defined functional relationships between the components of the authentication system and their role in ensuring the integrity, irrefutability of authorship and verification of electronic data. Content analysis was used to clarify the content of publications, international standards, and analytical reports that have become the scientific basis for writing a paper. The studies by C.L. Pedersen & T. Ritter (2024), S. Longpre *et al.* (2024) and I. Khomych *et al.* (2025) were analysed. The analysis has enabled the systematisation of current approaches to the verification of digital content and the identification of general risks directly associated with the automated generation of information.

The technical specifications of the Coalition for Content Provenance and Authenticity were considered (2024), which offered a model for cryptographic recording of the origin of digital content, and the ISO/IEC 42001:2023 (2023) standard, which defines the features of risk management, responsibility and transparency of the use of AI systems. The analytical basis of the study was supplemented by data from the European Union Agency for Cybersecurity (2023), which records trends in the growth of cyber threats associated with the use of generative technologies. Materials from the Council of Europe (n.d.a; n.d.b) were used as sources of official normative texts. The method of scientific generalisation substantiated approaches to improving the procedures for confirming the origin, integrity, and reliability of electronic documents, considering current risks and threats to information security caused by the use of an artificial intelligence system.

Results and Discussion

Methodology for detecting generative content in electronic documents

In the context of global digital transformation, there is a change in the principles of perception of reality due to the fusion of physical and virtual environments. Humanity has entered a new phase of digitalisation, where the line between the artificial (created with the help of digital technologies) and the authentic (connected with material reality) becomes less noticeable. C.L. Pedersen & T. Ritter (2024) stated that the created pseudo-authenticity is not based on the actual reliability of information, but on its perceptual reality, which is built on the visible connection between the digital entity and the individual, place, and time. This state of affairs forms a new information paradigm, within which truth takes on a relative character, and trust in digital content depends mainly on technical and visual features, and not on its objective compliance with reality. The researchers confirmed that contemporary AI-based systems achieve a high level of digital authenticity, that is, synthetic pseudo-reality is perceived as real and true. This creates new authentication requirements for artefacts, interactions, and data sets associated with or authorised by a person or organisation.

Artificial intelligence systems generate three different forms of results: artefacts (text, images, audio,

and video), interactions, and data sets that cannot be distinguished from "intelligent" information created by humans. In addition, advanced digital technologies can interact with users in such a way that the latter perceive these interactions as communication with real people. This phenomenon is a separate dimension of digital authenticity, which is characterised as "interactions generated by artificial intelligence", that is, social and communicative processes of reproducing signs of human behaviour using algorithmic and generative technologies. According to C.L. Pedersen & T. Ritter (2024), another component of generative AI is the development of a set of synthetic data that has the same properties as real-world data, but is autonomous, which is united by one characteristic – "to appear real and true", based on the inability to distinguish between human and machine origin. To form a full-fledged system for determining the origin of data in digital environments, researchers use a number of specialised approaches aimed at ensuring the attributability and traceability of information. These approaches include authentication methods for content and related metadata that are recorded during the creation and dissemination of information; consent and refusal registration mechanisms that allow authors to determine the terms of use of their materials; standardised formats for documenting the origin of data sets; and specialised libraries and registries that aggregate information about data sources and characteristics. The use of these tools helps to give unstructured data attributes, verify their authenticity, and provide navigation in formats suitable for machine interpretation. As noted by S. Longpre *et al.* (2024), none of these approaches alone provides a comprehensive solution to the problem of data origin in artificial intelligence systems, since they mainly focus on verifying the source or reliability of information and do not fully cover such critical aspects as copyright, licensing conditions, confidentiality, and legal regime of data use.

According to A. Farooq & C. de Vreese (2025), in the context of disinformation generated by AI systems, content authenticity is a central category for determining its credibility. According to scientific research by the Coalition for Content Provenance and Authenticity (2024), authenticity is a property of digital content that contains a set of origin and connection data that can be cryptographically verified for forgery. Generative neural networks built on a transformable architecture can create text, visual, and even structured documents similar to the originals. The use of such models for editing or full generation of official documents creates the risk of synthetic falsification, namely, forgery of content while maintaining external signs of authenticity. As a result, there is a threat to electronic document management systems (EDM). As noted in the European Union Agency for Cybersecurity (2023), attackers are increasingly using generative models to create documents that mimic corporate contracts, tax returns, or certificates.

European Parliament (2023) prohibits the placement, commissioning, and use of artificial intelligence systems that use subconscious influences aimed at circumventing a person's conscious control, and purposefully manipulative or deceptive methods, if their use is intended or leads to a significant distortion of the behaviour of an individual or group of persons due to a significant violation of their ability to make informed decisions, resulting in actions that would not have been taken in the absence of the influence of the relevant AI systems, which would have caused them significant harm. To counteract such risks, it is necessary to introduce mechanisms for verifying content by origin that record the history of edits and the source of document creation, for example, using Coalition for Content Provenance and Authenticity (2024) standards or integration with blockchain registries. For example, a digital watermark involves embedding a hidden and unique template or code in content during its creation, which can later be used to verify its authenticity. Blockchain technology offers another layer of security by providing a decentralised and immutable register of content creation and distribution, making it easy to track unauthorised changes. M.R. Shoaib *et al.* (2023) described an approach that uses biometric authentication, which uses unique biological characteristics such as facial recognition patterns, voice prints, or even print rhythms, to verify identity in digital media. However, these methods must balance the need for security with concerns about privacy and the possibility of abuse. Such challenges create the need to create a new digital trust architecture that combines legal, technical, and ethical mechanisms. This is not only about checking electronic signatures, but also about establishing the authenticity of the entire chain of content creation, processing, and publication. Such systems should be based on the principles of transparency, reproducibility, and confirmed origin of data. Despite the fact that conventional mechanisms for protecting electronic documents, in particular, qualified electronic signatures, cryptographic algorithms, certificates of trusted suppliers, remain the foundation of digital security, their effectiveness is gradually decreasing in the face of new threats generated by generative AI systems. Technologies that can create and modify information are becoming more powerful, which significantly complicates the verification of the authenticity of digital materials.

The introduction of more progressive and secure electronic signatures, such as biometric or multi-level signatures that provide maximum security and legal force of documents, will increase the level of protection against unauthorised access, prevent falsification of documents, and improve the legal weight of electronic documents. According to D. Tarasenko (2025), reducing the burden on employees, reducing the likelihood of errors, improving the efficiency of management processes can be achieved by introducing artificial intelligence technologies for automatic classification, processing and redirection

of documents, and for predicting the necessary actions based on data analysis. In particular, creating an ecosystem where data authenticity, consent, confidentiality, legality, and relevance are considered and managed holistically requires a unified data origin structure. In addition, the blockchain is a promising mechanism for creating immutable records of the origin of electronic documents. Registration of the document hash in a decentralised registry provides verified confirmation of its creation and integrity. Changes to the document automatically change the hash, making forgery or unauthorised modification virtually impossible. According to ISO/TC 307:2016 (2016), blockchain solution standards recommend their use in authentication chains, especially in government document management and legal registers. According to scientific research by D. Tarasenko (2025), it is blockchain technologies that can significantly increase the security and transparency of electronic document management, especially when working with important documents and transactions. The technology provides immutability and the ability to track changes in documents, which increases the level of trust in such systems.

Ukrainian legislation and international standards on the regulation of authentication, integrity and origin of electronic data

In Ukraine, the authenticity of electronic documents is ensured primarily through a qualified electronic signature and digital trust services. The Law of Ukraine No. 2155-VIII (2017) defines authentication as "an electronic process that allows verifying the electronic identification of an individual or legal entity and/or the origin and integrity of electronic data". The Law stipulates that a qualified electronic signature has the same legal validity as a personal signature, and has the presumption of compliance with a handwritten one. It is created based on a qualified certificate and issued by accredited trust centres under the supervision of the National Cybersecurity Agency. Additionally, the law provides for an electronic seal of a legal entity and an electronic time stamp for recording the moment of signing. In addition, the law states that electronic documents with QES cannot be declared invalid only because of the electronic format. Another Law of Ukraine No. 851-IV (2003) details the general requirements for electronic documents (structural details), noting that a document is considered legally significant if there is an electronic signature confirming its authenticity. S.V. Hubariev & O.O. Loviak (2022) noted that when using an electronic digital signature, a high level of security, data protection, and document authenticity is guaranteed. The research by M.V. Parasiuk (2025) also confirmed that the national legislation establishes the legal status and legal force of an electronic document, but there is no mandatory condition for identifying an electronic document as a means of proof – an electronic signature.

According to S.V. Hubariev & O.O. Loviak (2022), an electronic digital signature functions as a comprehensive cryptographic mechanism that combines encryption, hashing, and the use of a public key certificate. Encryption involves applying a special algorithm to an electronic message that converts it into an encoded form and makes it impossible to get acquainted with the content without the appropriate access key. Hashing consists of converting an array of data of any length into a fixed-size bit sequence, which allows quickly comparing data and checking its integrity during signature formation and verification. A public key certificate, in turn, is an electronic document that certifies the connection between the public key and a specific entity, contains information about the issuer of the signature, the validity period of the certificate and its purpose. These elements are implemented as interrelated components of an automated process in the process of integrating an electronic digital signature into electronic document management systems. When creating a document in the EDM, the system generates a hash function of the file, after which the signer imposes a signature using its private key, and the public key along with the certificate is added to the document structure or checked through an external service. For example, in corporate internal document approval systems, signing is carried out through integrated cryptographic modules that automatically check the validity of the certificate in the registry and record the timestamp. If changes are made to the document after signing, the hash value changes, which allows the system to immediately detect integrity violations.

In general, the legal regulation of the authenticity of electronic documents in Ukraine is based on a clearly defined system of electronic identification and trust services, the central element of which is a qualified electronic signature as a legally significant means of confirming the origin, integrity, and authorship of electronic data. National legislation ensures the legal equality of electronic and paper documents, establishes the presumption of QES reliability, and forms a high level of cryptographic protection through encryption, hashing, and key certification mechanisms. Simultaneously, the existing authentication model is primarily focused on confirming the will of the subject, and not on comprehensive verification of the origin and life cycle of digital content. At the international level, the authenticity of electronic documents is ensured by standards and regulations. The Regulation (EU) No. 910/2014 of the European Parliament and of the Council (2014) forms uniform rules for qualified electronic trust services, in particular, defines the legal equivalence of a QES with a handwritten signature and creates a single list of trusted providers at the level of the European Union. According to the provisions of the regulations, an improved electronic signature must be uniquely associated with the signatory, provide the possibility of its identification, be created using data for generating an electronic signature that is under the exclusive control of the signatory, and be linked to the signed data in such a way that any further changes can be recorded and identified.

A common feature in the Ukrainian and European approaches is that an electronic signature is considered not as a separate physical object, but as an integral part of an electronic document or transaction, which guarantees the authenticity of the signatory and their will. The essence of an electronic signature is to establish and confirm a person in a digital environment and give their actions legal force. In other words, an electronic signature serves as an element of digital identity, giving the signer a trusted status in digital transactions. As noted by I. Khomych *et al*. (2025), the electronic signature appears as one of the key components of this system: it provides authentication (identification), data integrity (guarantee of document immutability), and non-repudiation (inability to deny its authorship). In particular, through the use of cryptographic methods, an electronic signature guarantees authenticity (the ability to verify the identity of the signer) and the integrity of electronic documents (control of data immutability after signing).

An important initiative to ensure the authenticity and integrity of digital content is the Coalition for Content Provenance and Authenticity (2024), which offers a cryptographically secure chain of origin model that captures information about the creation, editing, and publication of digital materials in the form of metadata that can be verified. This creates a technical basis for distinguishing authentic electronic documents from synthetically generated or manipulated content. It is worth noting that the C2PA (Coalition for Content Provenance and Authenticity) specification has no direct legal force, its implementation is consistent with contemporary regulatory approaches to the responsible use of artificial intelligence and complements international standards in the field of electronic identification and management of AI.

The European Telecommunications Standards Institute (ETSI), the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) cover the formatting and verification of electronic signatures, seals, and timestamps. For example, ISO/IEC 20248:2022 (2022) define a digital signature scheme in barcodes to verify data, and a number of ISO standards describe digital watermark techniques. The ISO/IEC 20248:2022 (2022) standard is particularly relevant as a tool for institutional risk management related to the use of artificial intelligence systems. The spread of generative models significantly complicates the identification of the origin, integrity, and reliability of electronic documents, which increases the need for formalised mechanisms for controlling the creation, modification, and use of digital content. ISO/IEC 42001:2023 (2023) sets out requirements for the system management of AI application processes, including the definition of responsibility, documentation of decisions, data management and transparency, which creates the organisational basis for the implementation of technical authentication standards. In conjunction with ISO/IEC 20248:2022 (2022), the standard forms a holistic system of regulatory support for the authenticity of electronic documents in accordance with the risks posed by AI systems.

Another important regulation governing mechanisms for the protection of electronic documents is the Framework Convention on Artificial Intelligence (Council of Europe, n.d.b), which sets out the principles for the safe implementation of AI – human dignity, transparency, non-discrimination. Also adopted is the European Parliament (2023) Artificial Intelligence Act, which introduces the obligation to label AI content. The legislation on digital services requires platforms to intensively monitor and identify manipulative content. Furthermore, UNESCO and OECD are developing ethical guidelines and calling for international cooperation in the fight against disinformation. Despite the activities of ISO, ETSI, and C2PA, there is no single international standard that would regulate the authentication of content created or modified using artificial intelligence. The available approaches are mostly fragmentary (Table 1).

Table 1. Approaches to content authentication in the context of artificial intelligence development and their application in electronic document management

Approach / Standard	Description	Application in electronic document management
eIDAS	European regulation on the authentication of electronic documents, in particular a qualified electronic signature (QES). Does not cover content created by AI.	Used to verify the authenticity of electronic signatures, but does not consider the possibility of manipulating AI-generated data, which can be a problem in the context of their growth.
ISO/IEC 42001	International standard of the artificial intelligence management system, which sets requirements for risk management, transparency, accountability, and control of the use of AI in organisations. Focused on the institutional level of management of the processes of creating and using AI systems.	Used for developing internal policies regarding the use of generative tools in the preparation of documents, fixing the source of content creation, and managing the risks of synthetic falsification. It does not provide automated recording of the modification history in EDM, but only forms general requirements for risk management.
C2PA	Technical specification that provides for cryptographically secure recording of metadata about the creation, editing, and publication of digital content (provenance data). Provides traceability of the chain of changes and the source of file origin.	Creates a technical basis for labelling content, but does not yet have legal recognition in most countries. Does not address the issue of authenticity in the absence or intentional deletion of metadata, nor does it cover the organisational context of using the document.

Source: Regulation (EU) No. 910/2014 of the European Parliament and of the Council (2014), ISO/IEC 42001:2023 (2023), Coalition for Content Provenance and Authenticity (2024)

Such a regulatory gap allows taking comprehensive responsibility for distributing forged documents created with the help of AI. For example, even if the generated content contains false data, there are no direct provisions in the current Ukrainian and European law regarding its labelling or prohibition of distribution without appropriate designations. This creates serious legal risks, as users and organisations cannot be sure of the legal purity of such materials and their responsibility for their use.

Information analytics as an integrative component of the contemporary electronic document audit architecture

Information analytics is gradually becoming the basis for security management in the digital content generation environment, including in electronic document management systems. It is an important component of the electronic document authentication architecture that links technical solutions (cryptography, digital signatures), regulatory requirements, and organisational processes (access policies, auditing, and risk management). In addition, analytics helps to establish the authenticity of content, track the origin of data, and counteract malicious use of generative AI. It is the information and analytical modules in the EDM that perform automated processing of event logs, metadata, and various versions of the document. The system compares timestamps, editing history, approval routes, and digital certificate statuses to identify discrepancies between the declared document creation procedure and actual user actions. For example, if a document was signed with a qualified electronic signature, but previously unauthorised interference or an unregulated version change was recorded, the analytical system generates an increased risk signal. This is consistent with the opinion of N. Zozulya *et al*. (2025), who considered information and analytical activities as the integration of algorithmic monitoring, anomaly analysis, and digital trace assessment into management processes. The researchers suggest that the use of analytical technologies enhances the ability of EDMs to identify the risks of digital content manipulation in a timely manner.

According to the generalisation by T. Kumarage *et al*. (2024), detection systems can analyse the statistical, stylistic, and structural features of a text to determine the probability of its machine origin. Integration of such algorithms into EDM allows evaluating the content of the document along with checking the signature and hash values. If, for example, in a corporate system, internal regulations provide for limited use of generative tools for creating service documents, the analytical module can compare the linguistic characteristics of a new document with the author's previous materials and identify atypical patterns. In this case, authenticity is considered not only as confirmation of the identity of the signatory, but also as compliance of the content with the established policies of the organisation. As noted by O. Fedoruk (2024), contemporary EDMs require integrated event monitoring mechanisms that allow detecting anomalies in document access, editing, and routing. Analytics modules process event logs, analyse atypical signing time intervals, repetitive operation patterns, or uncharacteristic user activity. The system can automatically record attempts at mass signing of the same type, non-regulatory version changes, or abnormal file movement between structural divisions. In other words, authenticity is evaluated not only through the validity of an electronic signature, but also through the compliance of the subject's behaviour with a typical business process model. As noted by V. Savchuk & V. Derii (2023), analytical mechanisms not only record events and technical parameters of documents, but also form an information basis for risk assessment, monitoring compliance with procedures, and ensuring the reliability of management decisions. D. Liudvenko *et al*. (2023) emphasised that the information security of EDM should be based on the principles of comprehensive control of the document life cycle. Analytics allows tracking the origin of data by comparing versions, creation times, software tools used, and changes in the file structure. If, for example, a service document passes the approval procedure, the analytical system analyses the logic of the sequence of actions. If a sequence break or misalignment of timestamps is detected, a risk signal is generated that allows reconstructing the context of document creation and determine whether a hidden modification occurred before the final signing.

According to the European Union Agency for Cybersecurity (2023), there is an increase in cases of using generative models to create fake business documents and phishing materials. In such circumstances, only formal verification of the electronic signature does not guarantee the accuracy of the document content. Analytics allows performing correlation analysis of user behaviour, signing frequency, atypical time intervals, or mass operations of the same type, which may indicate automated or malicious use of credentials. These risks are confirmed by the results of the study by J. Zhou *et al*. (2023). The researchers prove that synthetic content created by contemporary generative models is characterised by a high level of logical consistency and stylistic plausibility, which significantly complicates its identification as automatically generated. However, algorithmic detection systems show limited stability in the case of adaptive models, while human confidence assessment often depends on cognitive biases and the context of perception. P. Perapu (2025) suggests that contemporary analytical technologies use machine learning and behavioural analysis to collect and correlate data from various sources to detect anomalies and threats in a timely manner. Such tools allow correlating data with various security systems and cloud services to detect complex attacks, and speed up the localisation of threats by detecting atypical user behaviour and changes in traffic. In addition, according to the researcher, information and

analytical technologies control complex document transfer routes, data duplication, or attempts to export files without authorisation through integration interfaces.

In addition, information analytics combines artificial intelligence, digital expertise, and other tools to verify the authenticity of content. According to T. Kumarage *et al*. (2024), analytical platforms use machine learning algorithms to distinguish AI-generated text from human text. Such systems detect characteristic patterns, inaccuracies, or biases in AI and can estimate the probability of content generation by artificial intelligence. In general, analytical products combine multi-level analysis of visual, audio, and file features to create detailed reports with evidence of content manipulation. Combining these methods with the use of blockchain trails, digital signatures, and a well-established audit procedure can significantly reduce the risks of fraud. Thus, information analytics in audit systems of electronic documents acts as an integrative component that combines legal requirements, technical means of protection and procedural control mechanisms. Its application allows comprehensively assessing not only the formal validity of an electronic signature, but also the context of creating, processing, and using a document. The analysis of behavioural, structural, and content characteristics of digital objects ensures timely detection of anomalies and potential risks of falsification.

The results of the study showed that the conventional model of ensuring the authenticity of electronic documents, which is based mainly on the use of qualified electronic signatures, cryptographic hashing and key certification, in the context of the spread of generative artificial intelligence systems, is insufficient to comprehensively counteract modern forms of falsification of digital content. In contrast to the classical paradigm focused on confirming the will of the subject and the integrity of the document, the approach proposed in the study provided for the integration of the information and analytical component as an independent level of verification. The conclusions obtained are partially consistent with I. Khomych *et al*. (2025), who viewed an electronic signature as an element of digital identity and emphasised its fundamental role in building trust in electronic transactions. The researchers emphasised that cryptographic mechanisms guarantee the authenticity of the signer and the integrity of the document. The researchers focused mainly on the legal and technical aspects of electronic signature as an identification tool, while the problem of analysing synthetic content created by AI remained out of consideration. The results of this study expand their best practices, as they demonstrate the need to supplement cryptographic verification with analytical procedures for detecting signs of automated generation.

The problem of changing the nature of authenticity in the context of the new phase of business digitalisation was conceptually explored by C.L. Pedersen & T. Ritter (2024). The researchers argued that in the fifth phase of digitalisation, authenticity is increasingly determined by perceptual characteristics, rather than actual compliance with reality. The main provisions of their scientific research confirm the results obtained in the study, according to which generative models create content with a high level of "pseudo-authenticity", which makes it difficult to distinguish it from the original sources. Of particular significance is the study by S. Longpre *et al.* (2024), in which the researchers identified a systemic crisis regarding the authenticity, consent, and provenance of data in the field of AI. They argued that the lack of a transparent mechanism for recording, storing, and verifying information about the origin of a digital object undermines confidence in the results of algorithmic processing. The results of the study are consistent with the opinion of the authors, specify it, and also prove the feasibility of implementing mechanisms for fixing the chain of document creation and editing as a mandatory element of EDM.

The technical aspects of confirming the origin of digital content were developed in detail by the Coalition for Content Provenance and Authenticity (2024), which proposed a specification for a cryptographically secure metadata chain. It was established that the proposed standard forms an important technological basis for documenting the history of content creation. However, unlike C2PA, where the emphasis is mainly on technical implementation, this paper proves the need for regulatory integration of such mechanisms, since without legal recognition, data on the origin of a digital object, the conditions for its creation, authorship, time parameters, and the history of modifications do not acquire proper evidentiary value. A similar conceptual approach to the representation of secure generative AI was proposed by J. Collomosse & A. Parsons (2024), who formulated a model of the three pillars – origin, transparency, and fairness. The results obtained confirmed the importance of these components, but supplemented them with an element of information analytics as a system integrator between legal and technical components. Questions of algorithmic detection of AI-generated text were systematised by T. Kumarage *et al.* (2024), who reviewed methods for detecting and attributing machine-generated content. Their results indicate the limited stability of modern detectors in the case of adaptive generation models. This confirms the thesis of the current study that it is impossible to rely solely on technical detection as a universal authentication tool. The technical side of the problem of synthetic media was analysed by Y. Mirsky & W. Lee (2021), who proved the continuous improvement of deepfake technologies and the complexity of their reliable detection. The results obtained confirm their opinion on the escalation of the technological confrontation between generation and detection. A report by the European Union Agency for Cybersecurity (2023) showed an increase in the number of attacks using generative models to create fake documents and phishing materials. These data confirmed

the empirical validity of the study's conclusions about the need to move from a reactive to a preventive approach in the field of authentication.

Thus, contemporary research mostly considers the problem either from the technical or legal side. But the results of this study consist in the synthesis of these approaches through the inclusion of information analytics as an integrative component of the system for ensuring the authenticity of electronic documents. The proposed model allows moving from fragmented solutions to a comprehensive risk management system that considers legal norms, technical standards, and algorithmic mechanisms for detecting synthetic content.

Conclusions

In the context of the rapid spread of generative content created by artificial intelligence systems, the issue of ensuring the authenticity and reliability of electronic documents is becoming of strategic importance. Given the growing risk of falsified documents, forged electronic signatures, and synthetic text and graphic materials, several advanced technological solutions are used in the current practice, which form the basis of digital trust. The electronic signature remains a key tool for verifying the authenticity of documents in a digital environment. The use of cryptographic algorithms based on the public key ensures the integrity, inevitability, and legal significance of electronic documents. Ukrainian legislation on the authenticity of electronic documents is based on a combination of QES and trust services, which corresponds to EU approaches. However, insufficient regulation of the legal aspects of the use of generative technologies and the lack of unified technical standards for digital authentication create significant risks for national security, personal data protection, and the functioning of electronic document management. The growing number of cases of using generative AI for destructive purposes, such as creating fake materials or imposing fake electronic signatures, requires the urgent introduction of comprehensive legal, technical, and ethical control mechanisms. Solving this problem is a key factor in building trust in digital communications, ensuring cybersecurity, and protecting the information space as a whole.

Information and analytical support becomes a key component of monitoring the work of dangerous and potentially risky AI technologies, as it provides an opportunity to form transparent mechanisms for monitoring, auditing, forecasting, and making managerial decisions. Thus, the integration of information analytics with the processes of evaluating and regulating artificial intelligence is a necessary condition for ensuring information security, the reliability of electronic documents, and the stability of society to manipulative influences. The development of generative AI puts forward new requirements: countries around the world, including Ukraine, are guided by global standards for labelling and verifying content. That is why it is advisable to strengthen participation in international initiatives, such as the Council of Europe, International Organization for Standardization, International Electrotechnical Commission, Institute of Electrical and Electronics Engineers, in order to update the national regulatory framework in a timely manner in accordance with global trends.

Thus, ensuring the authenticity of electronic documents in the era of generative content should be based on an integrated approach that combines reliable legal norms, technical standards, and adaptive verification mechanisms. The introduction of QES, electronic timestamps, and blockchain, combined with the harmonisation of national legislation and international acts, creates the basis for maintaining trust in digital processes and effectively countering information manipulation in the age of artificial intelligence. Future research will focus on developing a methodology for the automated verification of the origin and authenticity of generative content, and on exploring the potential of AI for detecting forged or synthetic documents.

Acknowledgements

None.

Funding

The study did not receive funding.

Conflict of Interest

None.

References

[1] Coalition for Content Provenance and Authenticity. (2024). *C2PA technical specification*. Retrieved from https://spec.c2pa.org/specifications/specifications/2.1/specs/_attachments/C2PA_Specification.pdf.

[2] Collomosse, J., & Parsons, A. (2024). To authenticity, and beyond! Building safe and fair generative AI upon the three pillars of provenance. *IEEE Computer Graphics and Applications,* 44(3), 82-90.

[3] Council of Europe. (n.d.a). *Council of Europe and artificial intelligence*. Retrieved from https://www.coe.int/en/web/artificial-intelligence.

[4] Council of Europe. (n.d.b). *The Framework Convention on artificial intelligence*. Retrieved from https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.

[5] Ege, O., Cagal, M., & Bicakci, K. (2025). Usability of token-based and remote electronic signatures: A user experience study. *arXiv*. doi: 10.48550/arXiv.2505.18814.

[6] European Parliament. (2023). *Artificial Intelligence Act*. Retrieved from https://superintelligenz.eu/wp-content/uploads/2023/07/EPRS_BRI2021698792_EN.pdf .

[7] European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
[8] Farooq, A., & de Vreese, C. (2025). Deciphering authenticity in the age of AI: How AI-generated disinformation images and AI detection tools influence judgements of authenticity. *AI & Society*, 41, 493-504. doi: 10.1007/s00146-025-02416-5.
[9] Fedoruk, O. (2024) Security and protection of information in electronic document management systems: Improving the level of cyber defense. *Bulletin of the Book Chamber*, 4, 39-44. doi: 10.36273/2076-9555.2024.4(333).
[10] Hubariev, S.V., & Loviak, O.O. (2022). Electronic signature as a component of electronic legal transactions. *Scientific Notes of V.I. Vernadsky Taurida National University. Series: Legal Sciences*, 33(4), 18-23. doi: 10.32782/TNU-2707-0581/2022.4/03.
[11] ISO/IEC 20248:2022 "Information Technology. Automatic Identification and Data Capture Techniques. Digital Signature Data Structure Schema". (2022, June). Retrieved from https://cdn.standards.iteh.ai/samples/81314/001eea69a1964a5bbba364b3117865ad/ISO-IEC-20248-2022.pdf.
[12] ISO/IEC 42001:2023 "Information technology. Artificial intelligence. Management system". (2023, December). Retrieved from https://www.iso.org/standard/42001.
[13] ISO/TC 307:2016 "Blockchain and Distributed Ledger Technologies". (2016). Retrieved from https://www.iso.org/committee/6266604.html.
[14] Khomych, I., Shvets, A., Soroka, S., & Kuten, R. (2025). Study of the electronic signature as an element of digital identity. *Social Development and Security*, 15(3), 187-200. doi: 10.33445/sds.2025.15.3.17.
[15] Kumarage, T., Agrawal, G., Sheth, P., Moraffah, R., Chadha, A., Garland, J., & Liu, H. (2024). A survey of AIgenerated text forensic systems: Detection, attribution, and characterization. *arXiv*. doi: 10.48550/arXiv.2403.01152.
[16] Law of Ukraine No. 2155-VIII "On Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19/en/ed20171005#Text.
[17] Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management". (2003, May). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15/ed20220101#Text.
[18] Liudvenko, D., Tomilova-Yaremchuk, N., Khomovyi, S., & Krupa, N. (2023). Information security in the conditions of digitization of accounting. *Scientific Collection "InterConf+"*, 33 (155), 120-129.
[19] Longpre, S., Mahari R., Obeng-Marnu N., Brannon, W., South, T., Gero K., Pentland, S., & Kabbara, J. (2024). Position: Data authenticity, consent, & provenance for AI are all broken: What will it take to fix them? In *Proceedings of the 41st international conference on machine learning* (pp. 32711-32725). Vienna: Messe Wien Exhibition Congress Center.
[20] Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys (CSUR)*, 54(1), article number 7. doi: 10.1145/3425780.
[21] Parasiuk, M.V. (2025). Electronic (digital) evidence in civil proceedings. *Analytical and Comparative Jurisprudence*, 1(4), 387-392. doi: 10.24144/2788-6018.2025.04.1.60.
[22] Pedersen, C.L., & Ritter, T. (2024). Digital authenticity: Towards a research agenda for the AI-driven fifth phase of digitalization in business-to-business marketing. *Industrial Marketing Management*, 123, 162-172. doi: 10.1016/j.indmarman.2024.10.005.
[23] Perapu, P. (2025). Anomaly detection in user behaviour using machine learning for cloud platforms. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 11(3), 805-809. doi: 10.32628/CSEIT25113343.
[24] Regulation (EU) No. 910/2014 of the European Parliament and of the Council "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng.
[25] Savchuk, V., & Derii, V. (2023). Relevant analytics is a determining factor in effective management of the company's activities. *Herald of Economics*, 4, 104-117. doi: 10.35774/visnyk2023.04.104.
[26] Sharma, J., Carvalho, A., & Bhunia, S. (2026). Provenance of AI-generated images: A vector similarity and blockchain-based approach, *In 2026 IEEE 23rd consumer communications & networking conference (CCNC)*, Las Vegas: IEEE. doi: 10.1109/CCNC65079.2026.11366470.
[27] Shoaib, M.R., Wang, Z., Ahvanooey, M.T., & Zhao. J. (2023). Deepfakes, misinformation, and disinformation in the era of frontier AI, generative AI, and large AI models. In *2023 international conference on computer and applications (ICCA)* (pp. 1-7). Cairo: IEEE. doi: 10.1109/ICCA59364.2023.10401723.
[28] Sviatoshniuk, A.L. (2023). About peculiarities of using of electronic digital signature in conclusion of civil contracts in the Internet. *Odesa National University Herald*, 25(2(37)), 21-24. doi: 10.32782/2304-1587/2023-25-2(37)-4.
[29] Tarasenko, D. (2025). Electronic document management as a tool for managing information processes in a company. *Review of Transport Economics and Management*, 12(28), 182-187. doi: 10.15802/rtem2024/317890.

[30] Zhou, J., Zhang, Y., Luo, Q., Parker, A.G., & De Choudhury, M. (2023). Synthetic lies: Understanding AI-generated misinformation and evaluating algorithmic and human solutions. In *Proceedings of the 2023 CHI conference on human factors in computing systems* (pp. 1-20). New York: Association for Computing Machinery. doi: 10.1145/3544548.3581318.

[31] Zozulya, N., Stekolshchikova, V., & Shoturma, N. (2025). Information and analytical activities in the age of digital transformation: New tools and methodologies. *Scientific Works of the Interregional Academy of Personnel Management. Philology*, 1(15), 21-26. doi: 10.32689/maup.philol.2025.1.4.

Нормативно-правове регулювання та стандартизація механізмів забезпечення автентичності електронних документів в епоху генеративного контенту

Оксана Василинина
Викладач
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
36011, просп. В. Грицаєнка, 24, м. Полтава, Україна
https://orcid.org/0000-0003-0402-4627
Ольга Мізіна
Кандидат філологічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
36011, просп. В. Грицаєнка, 24, м. Полтава, Україна
https://orcid.org/0000-0002-1988-6353
Ярослав Блоха
Кандидат філософських наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
36011, просп. В. Грицаєнка, 24, м. Полтава, Україна
https://orcid.org/0000-0002-0799-1789

Анотація. Актуальність дослідження зумовлена зростанням ризиків фальсифікації цифрових документів, підроблення електронних підписів, маніпуляції метаданими та поширення синтетичного контенту, який підміняє зміст автентичних джерел. Метою дослідження було визначення теоретичних засад формування комплексної системи захисту електронних документів, що поєднує нормативно-правові, технічні та інформаційно-аналітичні механізми верифікації, в умовах зростання ризиків потенційно дестабілізуючих впливів систем штучного інтелекту. У статті розглянуто нормативно-правові засади, підходи та механізми забезпечення автентичності електронних документів в умовах стрімкого розвитку контенту, який генерують за допомогою систем штучного інтелекту. Було проаналізовано чинне законодавство України у сфері електронних довірчих послуг та документообігу, а також міжнародні стандарти eIDAS, ETSI, ISO/IEC, C2PA, які регулюють питання автентифікації, цілісності та походження електронних даних. З'ясовано особливості сучасних технологій автентифікації, зокрема кваліфікованого електронного підпису, електронної печатки, блокчейну, цифрових водяних знаків, криптографічних хешів і механізмів фіксації походження контенту. Визначено специфіку впливу генеративного контенту на створення фейкових документів, синтетичних медіа та дезінформаційних кампаній. Схарактеризовано особливості інформаційної аналітики як ефективного інструменту виявлення, оцінювання та мінімізації ризиків, які безпосередньо пов'язані з використанням генеративного контенту в електронних документах. Обґрунтовано, що інформаційно-аналітичні методи дозволяють здійснювати багаторівневий аудит походження даних, аналіз метаданих, ідентифікацію ознак автоматизованої генерації та прогнозування загроз для систем цифрової довіри. Запропоновано розглядати інформаційну аналітику як інтегративний компонент сучасної архітектури автентифікації електронних документів, що поєднує правові, технічні та організаційні механізми забезпечення захисту інформації в умовах цифрових змін. Практичне значення дослідження полягає в можливості використання результатів для впровадження комплексного підходу до автентифікації даних у системах електронного документообігу. Крім того, запропоновані підходи до аналізу походження контенту, метаданих і ознак генеративної обробки уможливлюють створення систем моніторингу та аудиту електронних документів з метою виявлення фальсифікацій, синтетичних матеріалів і маніпулятивного контенту

Ключові слова: захист інформації; кваліфікований електронний підпис; метадані; системи штучного інтелекту; стандартизація; інформаційна аналітика