ИНФОРМАТИКА И КОМПЮТЪРНИ НАУКИ
INFORMATICS AND COMPUTER SCIENCES

LEGAL NATURE AND FEATURES OF THE TYPES OF ELECTRONIC SEALS

Milen Gospodinov
University for Library Studies and Information Technologies

Abstract: *This article examines the legal framework and practical applications of electronic seals as established by EU Regulation No. 910/2014, emphasizing their significance in ensuring the authenticity and integrity of electronic documents and transactions. By distinguishing electronic seals from electronic signatures and timestamps, the study delineates their unique features, including the classification into simple, advanced, and qualified types. The analysis further explores the role of electronic seals in enhancing cybersecurity within the digital environment. The findings highlight the pivotal function of electronic seals in digital transactions, underscoring their contribution to the reliability and security of electronic documents in the European digital single market.*
Keywords: *electronic seals, electronic signatures, cyber security, eIDAS, trust service*

1. NOTION OF ELECTRONIC SEALS

In the evolving digital landscape, the integrity and authenticity of electronic transactions have become paramount. The European Union, recognizing this need, established a comprehensive legal framework through EU Regulation No. 910/2014, also known as eIDAS, to govern electronic identification and trust services, including electronic seals. This article aims to dissect the legal nature of electronic seals, delineating their characteristics, classifications, and the role they play in securing digital documents and transactions. Unlike electronic signatures, electronic seals are specifically designed for use by legal entities, ensuring data integrity and origin authenticity with legal recognition across the EU. By examining the different types of electronic seals–simple, advanced, and qualified–the study sheds light on their practical applications and underscores their significance in enhancing cybersecurity measures. Through a detailed analysis of the regulation and its implications for the digital single market, this article contributes to a deeper understanding of electronic seals and their essential function in the digital age.

Regulation (EU) No. 910/2014, unlike Directive 1999/93/EC, introduces several new legal concepts related to electronic signatures. These concepts include electronic seals, electronic identification, electronic time stamp, website authentication, and electronic registered mail. These additions aim to enhance trust in cross-border electronic transactions in EU member states.

To better understand electronic seals, it is essential to consider them within the broader context of similar legal institutions outlined in Regulation (EU) No. 910/2014 and distinguish them based on their specific characteristics.

According to Article 3, item 25 of Regulation (EU) No. 910/2014, an electronic seal is defined as “data in electronic form, attached to or logically associated with other data in electronic form,

ensuring the origin and integrity of the latter" (Regulation (EU) No. 910/2014). The regulation does not explicitly define a "basic seal", but it can be deduced from the general definition provided earlier.

Furthermore, Article 3, item 29 introduces the concept of a "certificate for an electronic seal", which is an electronic attestation linking electronic seal validation data to a legal person and confirming their identit (Regulation (EU) No. 910/2014).

Another term defined in Article 3 of the regulation is the "advanced electronic seal". An advanced electronic seal must meet specific requirements outlined in Article 36. According to Article 36 of the Regulation, the advanced electronic seal must meet the following conditions:

(a) it is uniquely linked to the creator of the seal;

(b) it is capable of identifying the creator of the seal;

(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable (Regulation (EU) No. 910/2014).

Finally, the regulation defines a "qualified seal" in Article 3.27 as an advanced electronic seal created by a qualified electronic seal creation device, based on a qualified certificate for electronic seal.

The regulation defines two main functions specific to electronic seals. Art. 59 of the preamble of Regulation (EU) No. 910/2014 exclusively states that electronic seals should serve as proof that an electronic document was issued by a legal entity, guaranteeing the reliable origin and integrity of the document.

2. DIFFERENTIATION FROM SIMILAR REALMS

Electronic seals occupy a major place among other similar legal institutes from Regulation (EU) No. 910/2014. By their nature, electronic seals are closest to electronic signatures. In the Regulation, electronic seals provide the same legal possibilities as electronic signatures. For example, Regulation (EU) No. 910/2014 provides in Recital 58 that when a transaction requires a qualified electronic seal from a legal entity, the qualified electronic signature of the authorized representative of the legal entity should be accepted equally. Likewise, Art. 36, point 3 of the Regulation mandates that a qualified electronic seal based on a qualified certificate issued in one Member State is recognized as a qualified electronic seal in all other ɱember ѕtates. Additionally, both trust services are admissible as evidence in legal proceedings.

In addition to the many similar legal requirements between the two institutes, electronic seals and electronic signatures share the same technology. In this regard, it should be noted, for example, that qualified electronic seals carry the technical characteristics of a qualified electronic signature (Schwalm 2015).

Despite the relatively widespread adoption of trust services in e-commerce, there is still a slight mistrust of e-seals over e-signatures due to the latter's wider distribution and longer history. An objective assessment requires comparing the two institutes and highlighting the advantages of electronic seals over electronic signatures.

"Electronic seals can be used to seal any type of digital data, not just standard documents. It can secure software codes or servers, satellite images, cadastral plans, in fact, any kind of data prone to misappropriation or modification" (LuxTrust). Yet as a practical application, electronic seals today are mainly used for so-called "code signing". According to Recital 65 of Regulation (EU) No. 910/2014 "in addition to authenticating a document issued by a legal entity, electronic seals may be used to authenticate digital assets of a legal entity, such as software code or servers" (Regulation (EU) No. 910/2014). Code signing is the process of digitally signing executable files and scripts to verify the author of the software and ensure that the code has not been altered or corrupted after it

has been signed by using a cryptographic hash (Dumortier 2016).

As other additional examples of use in addition to those mentioned above can be such documents as tax and pension certificates or certificates and other certified documents that are issued and sent electronically (Dönnebrink 2021).

One of the most significant differences between electronic seals and electronic signatures is rooted in their functions. Electronic signatures are characterized by the functions of integrity, authenticity, confidentiality, and irrevocability (Dimitrov 2013), while electronic seals feature data integrity and authenticity features.

The first function of electronic seals is integrity or data integrity. Data integrity is maintaining and ensuring the accuracy and consistency of data throughout its lifecycle (Boritz 2005). It ensures the security of the data and guarantees its immutability over time after applying an electronic seal. By sealing documents with electronic seals through a content encryption process, the aim is to preserve the integrity of the data and ensure that it will not be altered at a later time. Furthermore, there is no certainty with electronic documents as to whether they have been altered (thus affecting their integrity) during their transmission path or while they are stored (Roßnagel 2013).

The second characteristic function explicitly stated in Regulation (EU) No. 910/2014 is authenticity. In fact, electronic seals were created in the current Regulation (EU) No. 910/2014 to replace the electronic signatures of legal entities used in the previous Directive 1999/93/EC. The purpose is to verify that a document really originates from a specific entity, thus ensuring its authenticity. For example, the fact of issuance (e.g., insurance certificate, permit) can be proven with an electronic seal. When it comes to electronic seals, this function ensures that the signed electronic document has not been tampered with after the electronic seal has been placed on it (Commission Staff Working Paper).

Ensuring the reliable authenticity of a particular document from a given legal entity is another distinctive function of e-sealing. This feature ensures that certain data originates from a specific legal entity or organization. After the electronic documents are stamped, the origin of the documents can be traced, i.e., from which legal entity they originate.

Another main distinguishing line between the electronic signature institute and the electronic seal institute is that the electronic signature refers to a natural person, and the electronic seal is used only for legal entities.

The protection in the use of this technology is based on the need to protect the information. The security of information is crucial to avoid its vulnerability, hence the importance of guaranteeing its availability (legal access to the information within the time limits established by its owner), its confidentiality (which excludes disposal of persons or unauthorized use), and its integrity (referring to its immutability) (De Miguel Asensi, PA 2002).

Electronic seals are very close to electronic signatures and share many common characteristics, but at the same time, have their own specifics, which makes them unique among other trust services.

Electronic seals also have similarities with electronic timestamps. Both institutes are data in electronic form that link other data in electronic form. However, with electronic timestamps, these are tied to a specific point in time and provide proof that the most recent data existed at that point in time, while with electronic seals, they are logically linked to data in electronic form to ensure its authenticity and integrity. Another similarity is that along with electronic signatures, electronic seals, and electronic timestamps are admissible as evidence in court proceedings. In addition, one of the requirements of a qualified electronic timestamp under Regulation (EU) No. 910/2014 is that it is signed with an advanced electronic signature or stamped with an advanced electronic seal of a qualified trust service provider or another equivalent method.

Electronic seals occupy their special place among other similar legal institutions of Regulation (EU) No. 910/2014, which distinguishes them from them, although they share common

characteristics with some of them. They have their specific role in commercial exchange, which is why their importance will grow more and more in the future.

3. TYPES OF ELECTRONIC SEALS

According to Regulation (EU) No. 910/2014, electronic seals are categorized into basic electronic seals, advanced electronic seals, and qualified electronic seals.

3.1. Basic electronic seals

Electronic seals, along with electronic signatures, are widely researched and used in two scientific fields – legal sciences and information technology (Menke 2009). The definition of a basic electronic seal is derived from the general legal definition of an electronic seal in Regulation (EU) No. 910/2014. It is described as "data in electronic form that is added to other data or logically linked to them to guarantee the origin and integrity of the latter." Similar to electronic signatures, the holder of the electronic seal is required to use it for signing.

3.2. Advanced electronic seals

The definition of an advanced electronic seal, as stated earlier, aligns with the requirements defined in Article 36 of Regulation (EU) No. 910/2014. According to this article, an advanced electronic seal must meet the following conditions:

(a) Unique linkage to the creator of the seal. (b) Capability to identify the creator of the seal. (c) Creation using electronic seal creation data that is under the control of the creator. (d) Linkage to the associated data to ensure the detectability of any subsequent changes.

Unique connection to the creator of the seal is a fundamental requirement for an advanced electronic seal. The seal creator refers to the legal entity that creates the seal. It is crucial to ensure there is no confusion regarding the identity of the legal entity associated with the electronic seal. Authentication can be established through a PIN code or specific username and password. Another essential condition is the ability to identify the creator of the seal unequivocally. This identification provides legal certainty about the entity behind the advanced electronic seal. The third requirement is that the seal should be created using electronic seal creation data that is under the control of the seal creator. The regulation does not specify the technology for creating this data. Finally, the advanced electronic seal must be designed to detect any subsequent changes made to the associated data. Various encryption technologies, such as asymmetrical keys and certificates, are employed to ensure data integrity (Dimitrov 2014).

The advanced electronic seal and the advanced electronic signature share many similarities, but they are primarily used by different entities. The advanced electronic seal is used by the creator of the seal or the legal entity, while the advanced electronic signature is used by the holder of the signature, a natural person who creates the electronic signature. Both types provide a high level of control and traceability.

3.3. Qualified electronic seal

The qualified electronic seal is the highest level of judicial power and commonly used. In accordance with Article 3.27 of Regulation (EU) No. 910/2014, it is considered an advanced electronic seal and must meet two additional requirements:

1. Created by a device specifically designed for creating qualified electronic seals.
2. Based on a qualified electronic seal certificate.

According to Article 3.31, an "electronic seal creation device" refers to configured software or hardware used to create an electronic seal. Qualified electronic seals offer a higher level of protection against tampering or data falsification. The device does not necessarily need to be physically held

by the seal creator and can be controlled remotely by a qualified trust service provider using techniques like PIN codes.

Annex III of the Regulation defines the conditions that qualified electronic seal certificates should meet. These conditions include appropriate indications, an unambiguous representation of the qualified trust service provider, details about the creator of the seal, validation data, certificate validity period, identity code, and other relevant information.

CONCLUSION

eIDAS (Regulation (EU) No. 910/2014) establishes the principle of mutual cross-border recognition of electronic seals. Article 35.3 states that a qualified electronic seal, based on a qualified certificate issued in one-member state, should be recognized as a qualified electronic seal in all other member states. This provision ensures the seamless use of qualified electronic seals in cross-border transactions within the European Union, facilitating electronic trade.

Since the implementation of Regulation (EU) No. 910/2014, the use of electronic seals has increased, and their significance in cross-border electronic transactions within EU member states continues to expand. They play a vital role in ensuring cyber security and protecting data from external influences.

REFERENCES

Boritz, J. (2005). "IS Practitioners' Views on Core Concepts of Information Integrity". *International Journal of Accounting Information Systems. Elsevier, Volume 6, Issue 4 , December 2005, pp*. 260–279.

***COMMISSION** STAFF WORKING PAPER, IMPACT ASSESSMENT Accompanying the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* on electronic identification and trust services for electronic transactions in the internal market, /* SWD/2012/0135 final – COD 2012/0146 */, (2012). [viewed 01 February 2024]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0135.

DE MIGUEL ASENSIO, PA. (2002). *Derecho privado de internet*. Madrid, p. 383.

Dimitrov, G. (2014*). Information and Communication Technologies Law,* Volume I – Civil Law Aspects, Law and Internet Foundation, Sofia.

Dimitrov, G. (2013). *Liability of Certification Service Providers.* VDM Verlag Dr. Mueller, Saarbruecken, 330 p.

Dönnebrink, M. (2021). Produktblatt Qualified Seal ID – Fortgeschritten elektronisch siegeln. D-trust GmbH, Version 01.02.2021. [viewed 01 February 2024]. Available from: https://www.bundesdruckerei .de/system/files/dokumente /pdf/Produktblatt-Qualified-Seal-ID.pdf.

Dumortier J. (2016). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). [viewed 01 February 2024]. Available from: http://dx.doi.org/10.2139/ssrn.2855484.

Dumortier, J. & N. **Vandezande** (2012). Trust in the proposed EU regulation on trust services? Computer Law & Security Review, 28(5), 568-576. [viewed 01 February 2024]. Available from: doi:10.1016/j.clsr.2012.07.010.

LuxTrust (2024) Electronic seal – enabling professionals to sign documents electronically on behalf of their companies,published: 24 June 2020. [viewed 01 February 2024]. Available from: https://www.digitalfuturemagazine. com/2020/06/24/electronic-seal-enabling-professionals-to-sign-documents-electronically-on-behalf-of-their-companies/.

Menke, F. (2009). *Die elektronische Signatur im deutschen und brasilianischen Recht,* Baden-Baden, p. 25.

Regulation (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive Directive 1999/93/EC. [viewed 01 February 2024]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT /PDF/?uri=CELEX:32014R0910.

Roßnagel, A. (2013). *Beck'scher Recht der Telemediendienste Kommentar.* München.

Schwalm, St., V. **Theresa** (2015). *Die Bedeutung der eIDAS-Verordnung für Unternehmen und Gehörden Neue Chancen und Herausdorfen für vertrauenwürdige elektronische Geschäftsprozesse in Europa BearingPoint GmbH*. Berlin.

ПРАВНА СЪЩНОСТ И ОСОБЕНОСТИ НА ВИДОВЕТЕ ЕЛЕКТРОННИ ПЕЧАТИ

Резюме: *Тази статия разглежда правната рамка и практическите приложения на електронните печати, установени с Регламент на ЕС № 910/2014, като подчертава тяхното значение за гарантиране на автентичността и целостта на електронните документи и транзакции. Като разграничава електронните печати от електронните подписи и електронните времеви печати, изследването очертава техните уникални характеристики, включително класификацията на обикновени, усъвършенствани и квалифицирани печати. Анализът допълнително изследва ролята на електронните печати за подобряване на киберсигурността в цифровата среда. Констатациите подчертават основната функция на електронните печати в цифровите транзакции, като подчертават техния принос за надеждността и сигурността на електронните документи в европейския цифров единен пазар.*

Ключови думи: *електронни печати, електронни подписи, киберсигурност, eIDAS, удостоверителна услуга*

Milen Gospodinov, PhD candidate
University of Library Studies and Information Technologies
E-mail: m.gospodinov@unibit.bg