BULGARIAN ACADEMY OF SCIENCES
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2025 • Vol. **83**, pp. 18-31
p-ISSN: 2738-7356; e-ISSN: 2738-7364
https://doi.org/10.7546/PECR.83.25.02

Operational Model of the Qualified Electronic Seals

Milen Gospodinov

University of Library Studies and Information Technologies,
119, Tsarigradsko *shosse Blvd. 1784 Sofia, Bulgaria*
email: m.gospodinov@unibit.bg

Abstract: The technical foundation of the qualified electronic seals is a complex realm, which requires considering many engineering aspects. To better understand their significant role in the digital world, as a relatively new concept introduced by Regulation (EU) No. 910/2014 (eIDAS), and to assess their economic feasibility, the operational model on which they rest, must be studied in connection with the principles of information security. The study is a review of the literature research in the field of information security and the technological aspects of the electronic signatures and the electronic seals. The analysis of the operational model of the qualified electronic seals has been elaborated in comparison to the qualified electronic signatures model. It is visualised through respective graph schemes which will trace the correlation between the principles of information security and their technological implementation. The qualified electronic seals are of particular interest to information security, and a thorough understanding of its operational model could lead to the implementation of measures to improve cybersecurity.

Keywords: electronic seal, electronic signature, PKI, cybersecurity**.**

1. Introduction and methodology used

Digital transformation has had a tremendous impact on the modern business environment, changing the way businesses interact with customers and consumers and fundamentally rethinking goals and strategies. Digital transformation affects various aspects of business, including technology, processes, culture, and customer relations, and reflects not only technological advances but also the introduction of new business management models [1, 2]. An integral part of this transformation are the technological aspects of qualified electronic signatures and qualified electronic seals, which play a key role in ensuring secure and trustworthy

digital interactions. Therefore, it is important to explore how the principles of information security influence their technological implementation. Understanding the technical operation of a qualified electronic seal (QES) primarily ensures that a sealed document has not been tampered with after sealing. Familiarity with cryptographic mechanisms, such as hashing and encryption, enables stakeholders to verify that these processes effectively protect data integrity.

While qualified electronic signatures are more commonly used, qualified electronic seals require greater attention as a less widely adopted tool for e-commerce. Understanding their operation builds confidence among users and entities relying on seals, particularly for cross-border digital transactions, where they are legally recognized under the EU eIDAS Regulation as strong evidence in disputes.

On the other hand, mismanagement or misunderstanding of QES operations – such as improper handling of private keys – can lead to breaches or misuse. As cyber threats continue to evolve, understanding the technological underpinnings of QESs enables organizations to adopt better practices for managing cryptographic keys and maintaining secure system.

Electronic seals (e-seals), along with electronic signatures, are widely researched by two scientific fields: legal sciences and information technology [3].

The *legal aspects* of electronic seals and signatures are just as significant as their technological aspects to achieve a comprehensive understanding of their practical use in the digital world. They are regulated by the Regulation (EU) No. 910/2014 on the electronic identification and trust services (eIDAS). Since one of the types of e-seals – the qualified e-seal, reveals highest degree of legal value and thus being the most preferred instrument by the market agents, it will be the focus of the analysis of this study.

The *technical aspects* of e-seals and their operational model are also examined herein below. It will become evident, that the e-seals play a crucial role in enhancing information security, especially in e-commerce [4].

For this paper, a comprehensive systematic literature review was conducted to gather data on the operational model of electronic signatures and the principles of information security. This information was then adapted to the context of qualified electronic seals. Primarily, electronic databases such as Google Scholar were searched to identify relevant resources and insights for the studied topic. Additionally, other internet resources, such as presentations of products offered by trust service providers and other similar, were also considered.

2. Legal basis of the types of electronic seals and the qualified electronic seals in particular

It is essential to clarify the legal basis of qualified electronic seals, along with other types of electronic seals, to fully comprehend the technological aspects of

this concept. Article 3.25 of eIDAS provides the legal definition of an electronic seal: “data in electronic form that is added to or logically linked with other data to guarantee the origin and integrity of the latter”. While this definition is generic, in theory, it is considered to be the definition of the “basic” e-seal. Depending on the level of security and the legal value vested therein, two other types of e-seals are regulated: the advanced and the qualified e-seal.

The definition of advanced electronic seals is introduced by Article 36 of Regulation (EU) No. 910/2014. In addition to the requirements of the basic e-seal, advanced electronic seals must meet the following conditions:

(a) They must be uniquely linked to the creator of the seal.

(b) They must be capable of identifying the creator of the seal.

(c) They must be created using electronic seal creation data that is under the control of the creator.

(d) They must be linked to the associated data in such a way that any subsequent changes to the data are detectable.

In comparison to the definition of advanced e-signatures introduced by Article 26 of eIDAS, the rules in Article 36 are largely identical. The only difference is that the term “creator of the seal” is used to refer to advanced electronic seals, while the term “signatory” is used for advanced electronic signatures. This distinction is well understood, as the advanced electronic signature can be linked to a natural person, while the advanced electronic seal can only be referred to a legal person.

Another notable distinction is that advanced electronic signatures must be “created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control” (Article 26(c)). In contrast, for advanced electronic seals, it is only specified that they should be “created using electronic seal creation data that the creator of the seal can, with a high level of confidence, use under its control for electronic seal creation” (Article 36(c)). Among the three types of e-seals, the qualified one is the most widely used. According to Article 3.27 of eIDAS, a qualified electronic seal shall be considered as an advanced electronic seal that further meets two additional requirements:

(a) It must be created by a device specifically certified for creating qualified electronic seals.

(b) It must be based on a qualified electronic seal certificate.

It should be noted that Article 38 of eIDAS mirrors the provision of Article 28, substituting “electronic signatures” with “electronic seals”, and refers to Annex III instead of Annex I. The key difference between the requirements set forth by Annex III and Annex I is that, with respect to the qualified certificate for electronic signatures, it must include “at least the name of the signatory or a pseudonym; if a pseudonym is used” (Annex I(c)), while for the qualified certificate for electronic seals, it must contain 'at least the name of the creator of

the seal and, where applicable, the registration number as stated in the official records' (Annex III(c))

3. Principles of information security relevant to the functioning of the qualified electronic seals

It is essential to examine the principles of information security, as they directly influence the operational model of qualified electronic seals.

The aim of information security is to ensure that an organization's hardware and software resources are used only for their intended purposes and within their designated frameworks. There are five fundamental principles in information security that every IT system must adhere to: integrity, confidentiality, availability, non-repudiation, and authentication. These principles are the cornerstones of cybersecurity for all IT systems. As an integral part of IT systems, qualified electronic seals must also comply with some of these principles.

3.1. Integrity

This principle ensures that data is not subject to unauthorized changes. According to researcher D. Gollmann, integrity involves preventing unauthorized modifications or alterations [5]. Loss of integrity can lead to fraud, poor decision-making, or other attacks. The system contains information that must be protected from unforeseen, unauthorized, or accidental modifications. Academic researcher W. Stallings divides integrity into two concepts: data integrity and system integrity.

- **Data Integrity**: Ensures that information (both stored and transmitted) and programs are altered only in a specified and authorized manner.
- **System Integrity**: Ensures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation [6].

The integrity principle is one of the key features attributed to qualified electronic seals. The technological sealing process ensures data integrity and prevents future attempts to alter the information. This is achieved through "integrity verification," which ensures that the sealed data remains intact. Asymmetric cryptographic methods are used to verify whether a sealed document has been changed.

At the moment of seal creation, a hash function is applied to the original data, and the computed digest is encrypted with the e-seal private key. This encrypted hash of the original data constitutes the e-seal. During verification, the relying party again derives the hash digest using the same algorithm employed at the moment of sealing. It is then compared to the one derived from the decryption of the e-seal with the public key listed in the e-seal certificate. If both values match, data integrity is confirmed, indicating no modifications.

3.2. Non-Repudiation

When a message is received, it is important not only to uniquely identify the sender but also to ensure that the sender assumes full responsibility for the information sent. Non-repudiation prevents the sender from denying authorship of a message. Scholar W. Stallings claims that non-repudiation ensures that neither the sender nor the recipient can deny the message transmission. This means the recipient can verify that the claimed sender did indeed send the message, and the sender can confirm that the recipient actually received it [6].

One of the requirements under Article 36 of eIDAS, applicable to the advanced electronic seal, is that it must be uniquely linked to the seal's creator. This condition also applies to the qualified electronic seal.

Non-repudiation is a key feature of the qualified electronic seal because the seal is tied to its creator and safeguarded by cryptographic methods. The use of a private key makes it impossible for the creator to deny authorship after the document has been sealed.

3.3. Authentication

Due to the insecure nature of communication channels, it is necessary to verify that the information received originates from the person who is genuinely believed to be the sender. According to N. Pohlman, authentication is the process of verifying whether a person or entity is genuinely the one they claim to be. It involves confirming the authenticity or identity of the subject [7].

As a qualified electronic seal uses Public Key Infrastructure (PKI), the legal entity behind the seal can be traced and authenticated. One of the primary functions of PKI is to verify digital certificates. The Certification Authority (CA) within PKI conducts verification procedures of the holder's data and ensures that their public key is genuine. This process enables the authentication of the legal entity that created the seal, confirming its identity and trustworthiness.

3.4. Confidentiality

Confidentiality refers to the protection of data from unauthorized access. Loss of confidentiality can result in data security issues, business losses, or a decline in credibility. The system contains information that needs to be protected against unauthorized disclosure. “Confidentiality of information assures users that their communications are safe and readable only by the intended recipients. Message encryption using electronic certificates assures this confidentiality” [8].

Confidentiality is not primarily an inherent feature of qualified electronic seals, as they are designed mainly to ensure data integrity, authenticity, and non-repudiation, rather than to protect the content of the document from unauthorized access.

3.5. Availability

Availability refers to the operational continuity of an information system. Loss of availability can lead to decreased productivity or damage to an entity's credibility. The system contains information or provides services that must be available in a timely manner to meet requirements or prevent significant losses. Availability is also not an applicable feature of qualified electronic seals.

4. Operational model of qualified electronic seals

Three main cryptographic concepts are used to secure technologically the operation of the qualified electronic seals:

1) Public Key Infrastructure (PKI): This involves the use of asymmetric key pairs (public and private keys) to ensure and verify the identity and authenticity of the entity creating the seal.
2) Hash Functions: These generate a unique hash value from the original document, ensuring integrity. Common hash functions include SHA-256 and SHA-3.
3) Digital Signatures: Created by encrypting the hash value of the document with the private key, ensuring non-repudiation. As common asymmetric algorithms could be used DSA, ECDSA, et al.

These concepts collectively enhance the security and trustworthiness of electronic seals.

4.1 The fundamental technology used for qualified electronic signatures and qualified electronic seals

The fundamental technology used for both qualified electronic signatures and qualified electronic seals is the public key infrastructure (PKI). A Public Key Infrastructure (PKI) is a system comprising software, hardware, and security protocols that facilitates secure information transfer over unsecured networks, such as the internet. It does this by employing two cryptographic keys: a private key and a public key, with the public key being issued by a trusted authority to authenticate identities and ensure safe data transmission [9]. The purpose of this infrastructure is to enable the secure and private exchange of data using two types of keys: a public key and a private key, both self-generated or obtained through a trusted third-party.

The private key is only accessible to the seal holder, while the public key should be made available to everyone. At one public key corresponds mathematically only one private key. The method's security relies on the near impossibility of deriving the private key from the public key, even using the most advanced computer systems within a feasible timeframe.

4.2. The sealing process of the qualified electronic seals

The sealing process of the qualified electronic seals is similar to the signing process with the electronic signatures, as they both employ common technology, including the use of hash algorithms. The process can be divided into two stages:

a) First stage: Sealing or Creation of a seal,
b) Second stage: Verification.

The process of e-sealing is based on the encryption with the private key and decryption with the public key of a given cryptographic value derived from the message, called a hash value. In the first stage, a digest of the message is created and encrypted. The message is hashed, and the result is signed with the seal creator's private key and appended to the message.

The one-way hash function generates a cryptographic checksum (hash value) from a message of a specified length. The formula used is:

$$h = H(M)$$

In this equation, h represents the checksum (hash value), H denotes the one-way hash function, and M indicates the message [10].

The sender generates a hash value based on the bits in the message and sends both the hash value and the message.

The second stage is the so-called verification, which encompasses the moment when the message is sent, and the recipient receives the sealed message. Upon receiving the sealed message, the message is separated from the seal, and the same hash function is applied to the message, obtaining a value $v1$. The recipient then decrypts the seal with the sender's public key, obtaining a value $v2$. If $v1 = v2$, and in case the newly derived hash matches the decrypted hash, the qualified electronic seal is authentic and the recipient is confident that the message has not been altered. The receiver then calculates the hash for the message bits and compares it to the received hash value. If the two values do not match, the receiver can conclude that the message (or the hash value) has been modified [11]. Once the electronic seals are generated, the private key-converted control numbers (the electronic seals) are added to or logically associated with the electronic statement, along with the issued qualified electronic seal certificate and a qualified timestamp (if applicable). Multiple file formats can be used for this process, including .docx, .xlsx, .pdf, .xml, .ps7, etc. The packet is then sent to the recipient [6].

4.3. Key components from Public Key Infrastructure

Both qualified electronic signatures and qualified electronic seals use digital signatures because they are a key component from Public Key Infrastructure (PKI). It's important to note that the term "electronic signature" differs from "digital signature" – the former is a legal term, while the latter is a mathematical and technical concept.

Anyone in possession of the sender's public key can verify that the message genuinely originated from the sender. The digital signature varies across documents: if A signs two documents, two different cryptograms will be generated. Likewise, if A and B sign the same document, they will produce different cryptograms.

When a message is sent from one party to another, the the receiver can verify the identity of the sender (associated with Authentication).The receiver has no means of tampering the message (associated with Integrity).

One key concern regarding the operating model of the qualified electronic seal is where the private key is stored. “A certified qualified signature creation device is required to store the personal key for a qualified seal. This can be a smart card or a hardware security module (HSM). The HSM can also be operated by a trust service providers offering a 'remote sealing service.' In this case, the activation of the e-seal by the legal entity must be ensured, though strong authentication of the respective user is not necessary” [12].

Fig. 1 illustrates the processes of creation of e-steal.

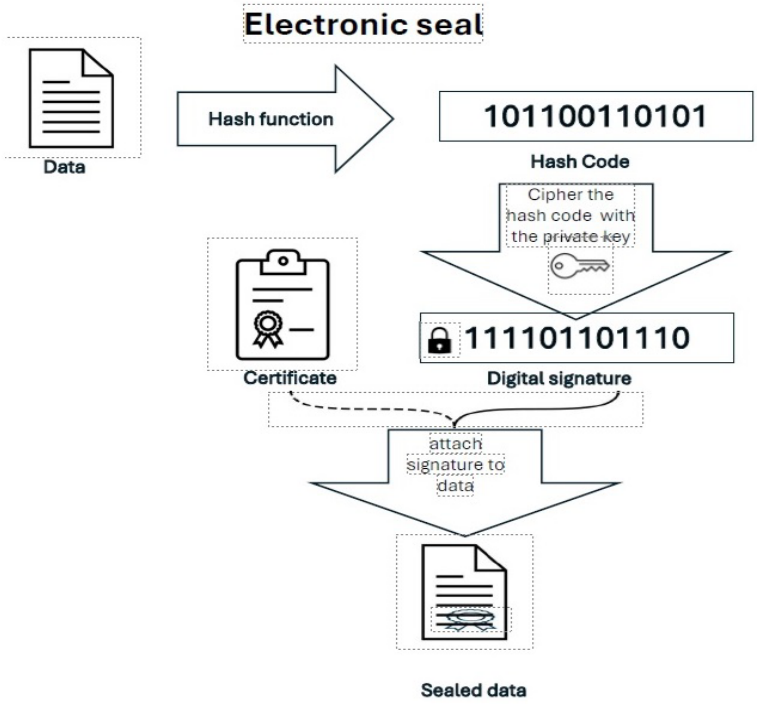

Fig.1. Creation of the e-seal

From a technological perspective, the creator of the seal cannot deny authorship (associated with non-repudiation) for the following reasons:

- The private key is under the exclusive control of the legal entity through cryptographic safeguards.
- Only the legal entity, via its Qualified Electronic Signature Creation Device (QSCD), can generate the seal.

This makes it technologically impossible for the creator to plausibly deny applying the seal, as the cryptographic process provides undeniable proof of authorship.

Regarding the processing method, it is worth noting that qualified electronic seals have a significant advantage over qualified electronic signatures because their operation can be automated [13]. On the other hand, the signing process typical of electronic signatures requires direct and active participation from the signatory.

Understanding the operational model of qualified electronic seals is of utmost importance because it clarifies the seal's technical and legal mechanisms, ensuring data integrity, authenticity, and non-repudiation. This knowledge enables entities to correctly apply and verify seals for the purposes of cross-border transactions, regulatory compliance and secure communications. Moreover, a thorough grasp of the model helps to identify the specific cryptographic processes that maintain the seal's integrity and establish trust in the sealed digital document or date.

Fig. 2 illustrates the processes of verification of e-steal.

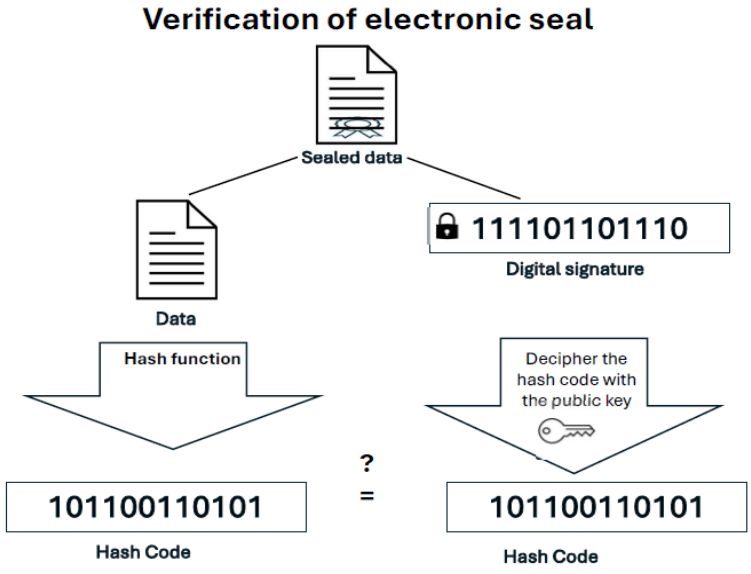

Fig.2. E-Seal verification

5. Electronic seal stadardazied formats

The qualified electronic seals can be linked to the sealed data in various standardized file formats, allowing for their integration with different types of documents and applications. Some of the commonly used file formats are:

a) XAdES (XML Advanced Electronic Signatures) – Specifically designed for XML-based data, this format provides extensions for electronic signatures, ensuring compliance with legal and technical standards.
b) CAdES (CMS Advanced Electronic Signature) – An extension of the Cryptographic Message Syntax (CMS) for electronic signatures, applicable to a variety of document types, where the seal is detached to the sealed data.
c) PAdES (PDF Advanced Electronic Signature) – A set of restrictions and extensions for PDF files that adapts them for secure electronic signatures.
d) ASiC (Associated Signature Containers) – This format specifies a container structure for storing signed data together with electronic seals, allowing them to be bundled with their signature format.

These formats ensure that qualified electronic seals can be effectively utilized across different platforms while maintaining their legal validity and technical integrity.

6. Validation services of a qualified electronic seal

Validation services are integral to the operational framework of qualified electronic seals, as they ensure that the seals meet regulatory standards, maintain integrity, and provide legal assurance in digital interactions. It is possible to apply validation services to both electronic signatures and electronic seals. They possess the mechanisms to verify the validity of the signatures or seals and confirm the status of the associated digital certificates.

Relying parties and third parties involved in electronic commerce must have certainty regarding the validity of the sealing process when a qualified electronic seal is affixed. Article 40 of eIDAS outlines the procedure for validating a qualified electronic seal in the same manner as a qualified electronic signature. Only a qualified trust service provider can confirm their validity. Article 32(1) of eIDAS describes the scope of validation applicable to both a qualified electronic seal and a qualified electronic signature:

a) The certificate supporting the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;
b) The qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
c) The signature validation data corresponds to the data provided to the relying party;

d) The unique set of data representing the signatory in the certificate is correctly provided to the relying party;
e) The use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
f) The electronic signature was created by a qualified electronic signature creation device;
g) The integrity of the signed data has not been compromised;
h) The requirements provided for in Article 26 were met at the time of signing.

Validation of a qualified electronic seal is a complex process that ensures the seal is created and verified in compliance with specific requirements. Here are the key steps involved in the validation process according to the ETSI TS 119 102-1 standard [14]:

1. **Seal Creation**: The qualified electronic seal must be generated using a secure device, typically a qualified electronic signature creation device (QSCD). This ensures the integrity and authenticity of the seal.
2. **Key Management**: The keys used for creating the seal must be managed securely. This includes generation, storage, and maintenance in a way that prevents unauthorized access.
3. **Seal Data**: The data constituting the seal should be structured according to the specifications laid out in ETSI standards, ensuring it includes necessary information about the signer, time-stamping, and the underlying characteristics of the seal.
4. **Signature Verification**: The verification process checks the integrity of the seal by confirming that the seal data has not been altered after creation. This typically involves validating the digital signature and its associated certificate.
5. **Certificate Validation**: The validation also includes checking the status and validity of the certificate used to create the seal. This may involve checking against revocation lists and ensuring that the certificate is within its validity period.
6. **Trusted Time**: If time-stamping is involved, the time-stamp must also be verified to confirm that the seal was created at a specific moment.
7. **Audit Trail**: Maintaining a secure audit trail, which includes logs related to the creation and validation process, can aid in compliance and verification of the seal.

These steps ensure that qualified electronic seals are not only secure but also reliable for legal and operational purposes. Overall, validation services play a vital role in the ecosystem of electronic signatures and seals, enhancing security, trust, and legal compliance in digital transactions.

Results: Based on the overview provided, it can be concluded that, out of the five principles of information security, three are applicable to qualified

electronic seals: **data integrity**, **authenticity**, and **non-repudiation**. Confidentiality and availability, as principles of information security, are not inherent to qualified electronic seals.

It is noteworthy how these principles of information security are technologically implemented in this type of eIDAS instrument:

- **Authentication**: Ensures the recipient can verify the identity of the sender. This is achieved through cryptographic keys, where the sender's identity is tied to a private key securely stored in a Qualified Signature Creation Device (QSCD), such as a smart card or Hardware Security Module (HSM).
- **Integrity**: Confirms that the message or document has not been altered during transmission or storage. This is ensured by generating a hash value (cryptographic checksum) of the document. Any modification results in a mismatch between the original and recalculated hash values.
- **Non-repudiation**: Prevents the creator of the seal from denying authorship. This is achieved through:
  - Exclusive control of the private key via cryptographic safeguards in a QSCD.
  - Binding the seal to the legal entity through a Qualified Certificate for Electronic Seal (QCSeal).
  - Cryptographic processes that provide undeniable proof of authorship, making it impossible for the creator to deny having sealed the document.

All these features can be summarized schematically in the following Table 1:

Table 1: Correlation of information security principles and their key technological mechanisms

Information security principle	Description	Key Technological Mechanisms
Authentication	Verifies the identity of the sender, ensuring the message or seal originates from the legitimate creator.	- Use of cryptographic keys (private key for sealing, public key for verification). - Storage of private key in a QSCD.
Integrity	Ensures that the message or document has not been altered during transmission or storage.	- Hash functions to generate cryptographic checksums. - Comparison of hashes to detect modifications.
Non-repudiation	Prevents the creator of the seal from denying authorship of the sealed document or message.	- Exclusive control of the private key through QSCDs. - Binding of the seal to the legal entity via QCSeal. - Cryptographic proof of authorship.

7. Conclusion

The operational model of the qualified electronic seals is one of the major cornerstones in understanding this type of realm of eIDAS, which is crucial for ensuring cross-border interoperability. Its technological importance is essential because it defines how the seal functions within a legal and technical framework. It encompasses the processes, protocols, and components that ensure the seal's authenticity, integrity, and non-repudiation. It enhances trust, ensures compliance, protects data integrity, and helps mitigate risk, all of which are indispensable components of a robust cybersecurity strategy. Therefore, a comprehensive overview and understanding of this model is necessary for addressing issues related to cybersecurity and providing safer communication between parties in the digital world.

References

1. Borissova, D., Naidenov, N., Yoshinov, R.: Digital transformation assessment model based on indicators for operational and organizational readiness and business value. In: Guarda, T., Portela, F., Diaz-Nafria, J.M. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2023. Communications in Computer and Information Science, 1935, 457–467, (2024), https://doi.org/10.1007/978-3-031-48858-0_36.
2. Borissova, D., Dimitrova, Z., Naidenov, N., Yoshinov, R.: Integrated approach to assessing the progress of digital transformation by using multiple objective and subjective indicators. In: Guizzardi, R., Ralyté, J., Franch, X. (eds) Research Challenges in Information Science. RCIS 2022. Lecture Notes in Business Information Processing, 446, 626–634, (2022), https://doi.org/10.1007/978-3-031-05760-1_37.
3. Menke, F.: Die elektronische Signatur im deutschen und brasilianischen Recht, Baden-Baden, ISBN 978-3-8452-1968-4, (2009).
4. Dimitrova, Z., Borissova, D., Mikhov, R., Dimitrov, V.: Group decision-making involving competence of experts in relation to evaluation criteria: Case study for e-commerce platform selection. In: Simian, D., Stoica, L.F. (eds) Modelling and Development of Intelligent Systems. MDIS 2022. Communications in Computer and Information Science, 1761, 42–53, (2023), https://doi.org/10.1007/978-3-031-27034-5_3.
5. Gollman, D.: Computer Security. 3-rd Edition, Wiley, 464 pages (2011).
6. Stallings, W.: Cryptography and Network Security: Principles and Practice. 7-th Edition, Pearson Education, Inc., Prentice Hall, (2006).
7. Pohlmann, N.: Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. Springer Vieweg, (2019).
8. Vacca, J. R.: Public key infrastructure: building trusted applications and Web services. Washington D.C.: Auerbach Publications, (2004).

9. Blanco, E.: Diseño y desarrollo de una aplicación Android para el uso de identidades digitales, autenticación y firmas digitaes en sistemas interactivos. (2014), http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20140519EvaMilagrosBlancoDelgado.pdf
10. Pohlmann, N., Hesse, M.: Kryptographie:Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (V) – Prüfsummen, Zertifikate und die sichere elektronische Signatur. DuD 31, 218–221, (2007), https://doi.org/10.1007/s11623-007-0076-2.
11. Dimitrov, G.: Legal Regulation of Digital Transformation. Dissertation, Sofia, (2023).
12. Göbel, C., Hühnlein, D., Kaiser, S., Entschew, E., Prummer, J., Schuster, M., Britze, N., Weiß, R., Schwalm, S., Michalek, T. M., Brand, T.: eIDAS und der ECM-Markt. Bitkom -Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2019), https://www.bitkom.org/sites/default/files/2019-06/190618_lf_ecm_eidas_web.pdf
13. Electronic signature vs electronic seal: main features and differences. (2024), https://focus.namirial.com/en/electronic-signature-vs-electronic-seal/.
14. ETSI TS 119 102-1 V1.2.1 (2018-08), Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services. (2018).