ACROSS
www.across-journal.com
Proceedings of the International Conference "Interdisciplinarity and Cooperation in Cross-border Research" Chisinau, Republic of Moldova, June 2022
Vol. 6. No. 1 – Economics

ELECTRONIC SIGNATURE AS A TOOL FOR IMPROVING THE EFFICIENCY OF PUBLIC PROCUREMENT

Ecaterina-Milica DOBROTĂ*, Marian STAN*, Mihai CIOBOTEA*, Viorel PÂRVU**

*The Academy of Economic Studies, Bucharest, Romania
**Independent researcher
Corresponding author: milicadobrota@yahoo.com

Abstract

The restrictions on the movement of persons imposed during the pandemic have highlighted that the whole process of awarding the public procurement contract can be carried out electronically (from identifying the need to signing the contract). One of the tools that can improve this process (as well as other operations adjacent to it) is the electronic signature. The purpose of this paper is to review the current state of play and examine to which extent (spread) the electronic signature is implemented and used, the benefits of them in public acquisitions, comparing with now (obsolete) handwritten signature. Using the electronic signature is an effective tool that did not reach its full potential. The qualified electronic signature (QES) offers multiple benefits in doing business with public organizations. Economic operators and public institutions/companies within EU countries will likely need to comply to be considered a party on a legitimate legal agreement. Our qualitative research on the current state of play of electronic signature market has revealed a number of key factors that influence the implementation and usage of this important tool for public acquisitions. The novelty of the paper is the analysis on usefulness of the electronic signature in the public procurement field. Starting from this article, research can be carried out to identify indicators for measuring the performance of the public procurement process carried out by public authorities, and the bidding activities.

Keywords: electronic signature, public procurement, digital platforms, intelligent economy

1. Introduction

Digitalization gains more and more in importance, the restrictions imposed by COVID-19 pandemics being the main acceleration engine for this phenomenon. The two-year online deployment of so many activities has revealed the necessity of transition toward the usage of informatics systems for collecting, processing and analysing of the information that we need (Suhail et al., 2021).

A set of operations which previously have required the physical presence of people, can be deployed now in online mode: the payment of taxes and various fees, sending declarations to public institutions, contract signing or any form of online shopping. The public procurement can be performed fully online as well, including all the acquisitions performed by a state-controlled entity.

The online transactions have raised various questions related to: data protection, the trust in the electronically sent documents, their validity and their legal status, the authenticity of the signatures, validating the person identity.

The EU Regulation no. 910/2014, also known as electronic identification and trust services (eIDAS) Regulation, establish the conditions of electronic identifications for persons, the applicable

rules for trust services related to electronic signatures along with the legal framework of the documents, seals and electronic signatures.

Subject to the type of the transaction/operation, on documents can be applied one of those three types of signatures: simple electronic signature (ES), the advanced electronic signatures (AES), the qualified electronic signature (QES), per Directive 2014/24.

Considering the definitions from article 3 from eIDAS regulation, we highlight the differences among these three types of signatures:

- **Electronic signature:** designates "data in electronic format, attached to or logically associated with other data in electronic format which are used by the signer to sign";
- **Advanced electronic signature (AdES):** designates an electronic signature that fulfils the four conditions from article 26, eIDAS Regulation:
  a) It references the signer;
  b) „It allows the identification of the signer";
  c) "Created using electronic signature creation data (a private key) that the signatory can, with a high level of confidence, use under his sole control";
  d) It is linked to the data used when signing in such a way that any subsequent change in the data is detectable.
- **Qualified electronic signature (QES):** defines "an advanced electronic signature which has been created by qualified electronic signature creation device and relies on qualified certificate for electronic signatures"; only this type of signature is explicitly recognized in all EU Member States as having the equivalent legal effect of a handwritten signature.

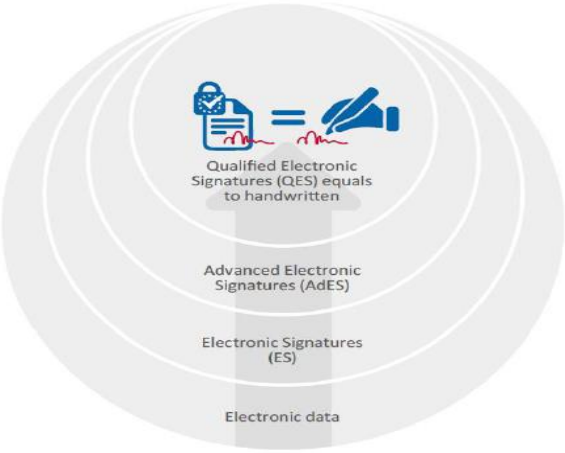

Figure no. 1 – Types of Electronic Signatures
Source: ENISA, 2016

According with article no. 22 from the Regulation no. 910/2014, each EU Member States has the obligation of publishing a single list - Trusted List - that includes the providers of electronic signature based on qualified certificates - trusted service providers (TPS).

A TPS represents a concept launched by European Parliament and European Council, via eIDAS Regulation and designates an entity that issue and maintain the digital certificates to create and validate the electronic signatures as well as authenticating the signatures and websites.

In EU, each member state has the obligation to create and maintain an up to date list of trusted service providers and their offers. In Romania, ADR- the Authority for the Digitalization of Romania - is the government entity that monitors the designated qualified trusted service providers. Furthermore, ADR has been designated to validate the unqualified trusted service providers in Romania.

At EU level, the complete list of qualified TPS is available at the following URL: https://webgate.ec.europa.eu/tl-browser.

The Figure no. 2 illustrates the distribution and the number of TPS in EU Member States.

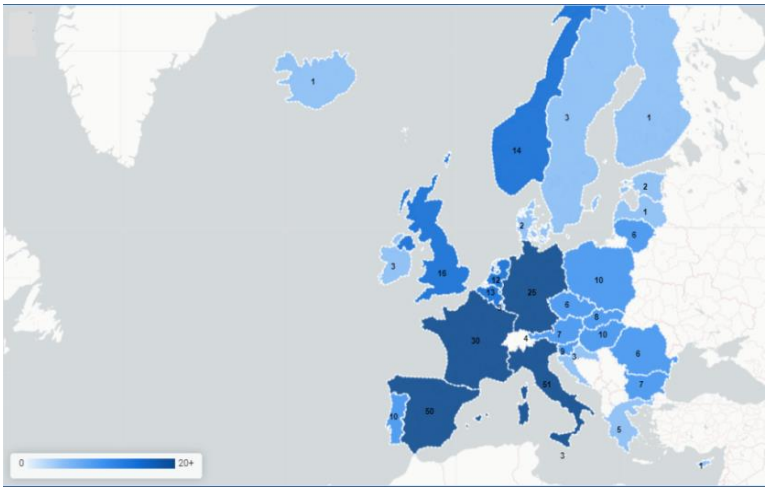

Figure no. 2 – Trusted Services Providers in Europe
Source: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/statistics

From the figure no.2 above, it can be seen that the highest numbers of trust service providers are from Italy (51), Spain (50) and France (30).

One of the domains in which the qualified electronic signature has an important role is the public acquisitions. According with the Directive no. 24/2014, the contracting authorities must deploy via electronic means any communication and assigning procedures of contracts that were initiated via advertisements. Since 2014, the utilization of the electronic means is mandatory both for buying entities (from the initiation of the procedure until the assigning of the contract) and for suppliers (from sending the offer until the signing of the contract).

The option of using the advanced/qualified electronic signature for such operations belong to EU Member States, subject to the level of security of the electronic means (as indicated in article no. 22 from the above-mentioned Directive). The application of this signature on the electronic documents significantly contributes to the efficiency of the entire process. Besides ensuring the integrity and confidentiality of the documents, the further benefits consist in substantially reducing the necessary material and human resources and the time allocated to this procedure.

In the current paper, the authors perform an analysis of the differences between these three types of electronic signatures (simple, advanced, qualified/extended) and their utilizations along with a study on the trusted service providers. A significant part from the paper is dedicated to the usages of electronic signatures in public procurement, presenting certain challenges that can occurs when implementing these signatures.

The article includes a section dedicated to the literature review, concerning the articles that have approached the topic of digital signatures, in interval 2019-2022. Another section is dedicated to results

and discussion regarding: the key factors that influence the implementation and the utilization of the electronic signature, the means of verification of electronic signature received from UE and non-UE providers; the problems that occur in utilization of electronic signature in public acquisition. Finally, the paper contains a section dedicated to conclusions, highlighting the originality of the research along with the recommendation for further research topics.

2. Review of the scientific literature and methodology

2.1 Review of the scientific literature

Document electronic transmission, data integrity insurance contained in these documents are these last years' subjects treated in numerous research papers in various activity fields. The identification of the articles containing these subjects was done by accessing Web of Science Core Collection, covering a multitude of research domains (Pranckutė, 2021). Searching the key words „digital signature" and „electronic signature" for the period 2019-2022, we received a list of 3,039 papers, respectively 6,609 papers, within diverse scientific categories (IT, medicine, economy, business, public administration, agronomy, religion, psychiatry, chemistry etc.) and from different countries. The most papers are from USA, China, Germany, UK, and France.

Regarding the applicable laws for electronic signature, EU Member States consider the Regulation 910 / 2014, and Romania considers Law 455 / 2001 regarding electronic signatures.

According with certain authors (Vatra, 2010), public key infrastructure at national level is an essential point in the development of public administration services. This will enable the citizens to secure electronic transactions with the national institutions. Other authors (Ruica et al., 2020) have proposed a technologically innovative way to use the existing cryptographic APIs (Application Programming Interfaces) and tool-kits to integrate remote digital signatures in a transparent way for the users and for the applications performing the actual signing.

Regarding public acquisitions, indications regarding the mandatory usage of the electronic signature are found in Law 98/2016 and application guidelines for this law, approved through HG no. 395/2016.

2.2 Methodology

For creating this paper, the authors searched for articles containing "electronic signature" published during 2019-2022 interval and found more than 6000 articles in Web of Science Core Collection; this fact alone shows a great interest in the subject.

The authors carried on the research by identifying the Romanian Qualified Signatures providers (QTSP), analysing the available public date on the EU/EU Trust Services Dashboard site. The authors also gathered some financial data for these providers from the site of the Romanian Ministry of Finance, as turnarounds for year 2020, analysing and comparing their activities.

In this paper, the authors used information, rules from the European directives and regulations, and also in national legislation. All information obtained were shown in graphs, in order to demonstrate the implication of the electronic signature providers in Extended Electronic Signatures implementation.

The paper is based on factual analysis of some cases solved by the National Council for Solving Complaints (NCSC), with the aim to demonstrate the issues, which can appear while using the Extended Electronic Signature.

3. Results and discussion

3.1. Analysis of trusted service providers in Romania

The eIDAS Regulation, article no. 26 indicates that he application of qualified electronic signature can be done if the signer has a signing device and a qualified certified from a qualified trusted service provider. The same Regulation (article no. 22) shows the obligation of the EU Member States to publish the list of qualified trusted service providers.

On EU website, under the section dedicated to Trusted List, in the page concerning Romania, there are six providers of the qualified electronic signature:

- ALFATRUST CERTIFICATION SA;
- CERTSIGN SA;
- CENTRUL DE CALCUL SA;
- DIGISIGN SA;
- TRANS SPED SA;
- Serviciul de Telecomunicații Speciale (STS).

From our analyses, we have removed the last provider from the list, STS , since this one is not a commercial entity but a non-profit governmental entity that provides services under special conditions, with low volumes and it does not significantly influence the market share of the other players, per our observations for 2020 (Figure no. 3).

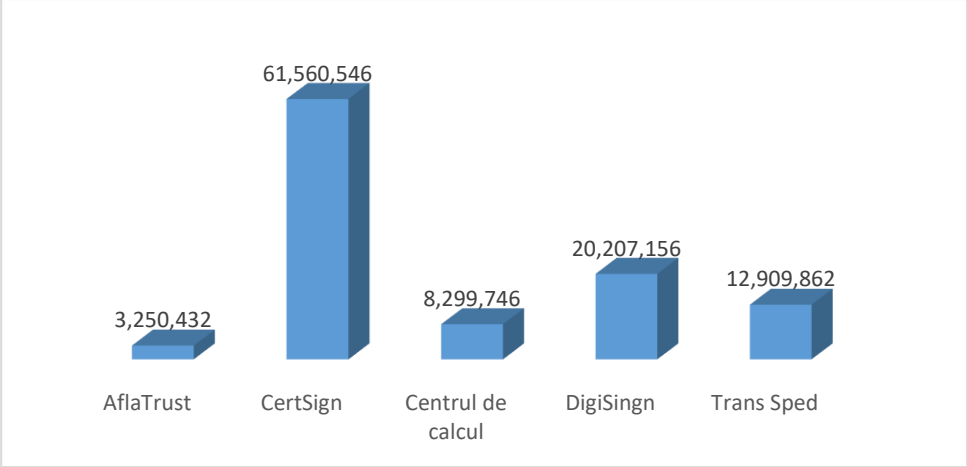

Figure no. 3 – The turnover of qualified electronic signature providers for 2020
Source: Authors, by using Ministry of Finance (2020)

The evolution of the electronic signature market in Romania, during 2017 – 2020 is a positive one (Figure no. 4) as the utilization of the electronic signatures has become the norm, even an obligation for certain activities (sending the financial statements, deploying the public acquisition process, etc.).

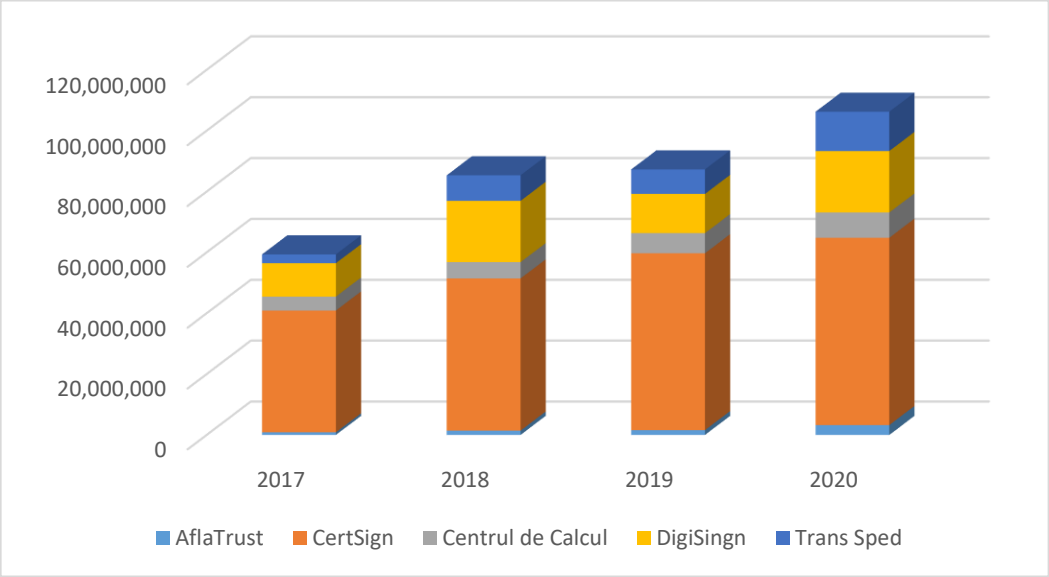

Figure no. 4– The evolution of the turnover for electronic signature providers during 2017-2020
Source: Authors, by using Ministry of Finance (2020)

3.2 Verification of the qualified electronic signatures (QES) from UE providers

One of the frequent questions raised by the recipients of the documents signed with QES is whether the documents have been signed based on certificate released by a trusted service provider.

From eIDAS Regulation, it has been mandated that, at EU level, the qualified trusted service providers to be listed in the Trusted List, that is published at CE level, on the following website: https://webgate.ec.europa.eu/tl-browser.

In this way, the QES issued based on a provider certificate that is included in Trusted List, is valid across EU Member States, including Romania.

In Romania, ADR is responsible for the publication of the updated Trusted List, including information regarding qualified trusted service providers (QTSP), on the website www.adr.gov.ro.

3.3 Verification of the qualified electronic signatures (QES) from non-UE providers

Taking into account that the signers of the electronic documents can be from outside EU, the question is how they can be internationally accepted the qualified electronic signatures issues by non-EU trusted service providers.

The answer to this question is in eIDAS Regulation (article no. 14) that indicates that the trust services coming from a third party/country are accepted at EU level based on an agreement between the EU and that country or international entity. With these agreements, it must ensure that the trusted service providers from the third parties and their services fulfil the same requirements as the EU providers. Further details regarding this issue can be found in the guide released by The European Union Agency for Cybersecurity - ENISA (2016).

3.4 Key factors that influence the implementation and the utilization of electronic signature

The economic activity is the basis for the development of society (Mândru and Săracu, 2021), the transaction closing would be easier if the electronic signature is used as a solution to remotely stamp the contracts. Using the „intelligent" contracts will significantly reduce the response time of the involved parties, the operational costs and the transactions middlemen (Kirillova et al., 2019).

On various domains such as public acquisitions or tax management, the activities cannot be performed if the documents do not have a qualified/extended electronic signature.

However, the implementation of the electronic signature is a challenge for many signing entities, being influence by a number of factors such as the training of the personnel, deployment of the national programs that sustain the utilization of extended/qualified electronic signatures, the level of involvement of the public organizations in the process of electronic signing.

The efficiency of the acquisition procedures is closely linked to the level of skills of the personnel involved both in the bidding process and in the writing of the assigning contract documentation and in the evaluation of the offers. Although the utilization of the electronic signatures in the process of public acquisitions seems to be an activity that does not require special knowledge (comparing with the knowledge level required by the job of public acquisition specialist), the practice has revealed the existence of a various problems. Some of them originates from the lack of the knowledge of the rules involved in the implementation of electronic signature or from the lack of the digital skills of the signers.

The training of the personnel that signs and loads the documents in SEAP (Sistemul Electronic pentru Achiziții Publice) will avoid the rejection of the offer or the incorrect application of the assigning procedure.

The deployment of national programs, which are meant to support the utilization of the extended electronic signatures, may accelerate the process of digitalization of both public administration and private companies.

The involvement of the public organizations represents a *sine qua non* condition for the deployment of these programs with an aim to implement the electronic signature in the day-to-day activities.

3.5 Legal value of electronic signature

Regarding the electronic signature, the public procurement legislation is related to the pre-contractual process only (from the initiation notice for procurement procedure to the communication of its result), that means it is used prior the procurement procedure. Thus, the manner of signing the contract is on the parties' free choice. The moving restriction of the future contractors, due to pandemic, in order to sign the contractual agreement in handwriting, has led to the transmission of their agreement by email or has resulted in the application of various types of signatures, assimilated to a private signature. However, an approach made available to the company (in general) and those involved in procurement (specifically) by technology as the existence of an electronic signature on a document in the public procurement process is not (yet) appreciated at the real value.

The electronic signature valences may not be limited only to findings on the non /existence of proof of the agreement of the person involved in issuing the signed act or to aspects of validation of the form of manifestation of this agreement (written form), but may be extended to the level of acceptance that its use gives additional guarantees to the premiums, in the sense that the user is identified and the content of the document, on which it is applied, is intact. The additional guarantees also result from the way the electronic signature is generated and verified, not only from the way it is communicated.

In order to keep up with technology, but also with the need to regulate the practical situations in which the use of electronic signatures may occur, the European Parliament and the Council (European Community regulators) have issued, inter alia, REGULATION (EU) NO. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

In order to easily understand the purpose of the widespread use of the electronic signature, it is relevant to go through the motivations in points 1, 2 but also 57 of this Regulation, related „building trust in the online environment", „enhance trust in electronic transactions" and „stimulate the private and public sector to invest in such services".

Despite that, the application provisions of Law no. 98/2016 use terminology that is not up to date with the European Regulation, it should be noted that, the use of electronic secure systems, in all public procurement procedures, is mandatory for the member states. Also, the acquis communautaire does not require the use of an electronic signature for public authorities.

According the aforementioned national regulation (Governmental Decision no. 395/2016), the contracting authorities and the economic operators are required to use the "extended electronic signature, based on a qualified certificate, issued by an accredited certification-service-provider (in a procurement procedure)".

On the other hand, the mentioned European Regulation defines this type of signature as a "qualified electronic signature" and means an advanced electronic signature which is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures (Article 3, para. 12).

The different terminology can be easily explained in relation to the evolution over time of national legislation (mainly the Law no. 455/2001) and European regulations, which mainly stands out that, any process that is based on an electronic signature must lead to the appreciation that it establishes and maintains users' confidence in online communications, including electronic transactions. To simplify the terms, further references will be made to the extended electronic signature.

The essential purpose of using the electronic signature may be undermined by the implementation of various national regulations, including those in the field of public procurement. On the one hand, excessive formalism, and on the other hand, the required online activity work tools (dedicated electronic platform, which has a high degree of cyber security) may lead to doubts about the practical usefulness of the required electronic signature.

However, the extended electronic signature, according to the national rules, must ensure trust to direct users, but also to indirect users (in the case of public procurement or bidders or public entities), by its characteristics, acquired at its creation and maintained during validity, including the case of amendments. According to the European regulation, that is equivalent to an advanced electronic signature based on a qualified certificate (see Article 26 and Article 27, about their characteristics).

The use of an advanced electronic signature based on a qualified certificate, from a legal point of view, is equivalent to any handwritten signature, in the sense that its opposability to the involved parties (signatory and recipient / recipient of the document) is similar in both cases.

Thus, once recognized by the signatory parties and those who oppose it, the document has full force, being considered an authentic document, and the written form of the document, imposed by a regulation such as procurement is fully assimilated by the electronic document, if it presents extended electronic signature.

Therefore, any document in the public procurement procedure that carries an extended electronic signature, is presumed to be authentic, in the sense that it is issued by its author/bearer of the signature,

for the purpose/for the scope of involvement in the procedure, to confirm the full content of the document, but also to guarantees its irrevocability and removal/limitation of the possibilities of altering its content. Anyone who denies this character of the electronically signed document must provide evidence to the contrary, the technical expertise being of maximum relevance (see art. 8 paragraph 1 of Law no. 455/2001: „If one of the parties does not recognize the document or signature, the court will always order that the checking must be done by specialized technical expertise.").

In the EU, the electronically signed document in one of the member states must be recognized by another member state, if the security guarantees for its issuance are equivalent to them, a rule which eliminates any dispute appeared as a result of differences in terms or national technical systems.

3.6 Issues that may occur when using the electronic signature in public acquisitions

In the public acquisition domain, the cyber security of all the information/documents, which are sent via electronic means of bidding, represents a concern both from UE level and from the assignment process participants' level. Following the security rules, such as those of authentication and preserving the integrity of information requires the utilization of the qualified electronic/digital signature (Farooq, Hussain, and Ustun, 2019).

The only electronic signature that can be equated with the handwritten one is the signature based on a qualified digital certificate, according with the Law no. 455/2001.

Performing public acquisitions through electronic means requires the utilization of a trust system for sending, keeping and analysing the data. The user authentication is one of the essential security requirements, taking into account the fact that data which is collected via electronic platforms are sensitive and sometimes confidential (Meshram et al., 2020). The extended electronic signature represents a key element that ensures data integrity, authentication and acceptance.

In Romania, the Law no. 98/2016 requires the electronic deployment of public acquisition procedures that are performed through the publicly available online platform - SEAP, www.e-licitatie.ro that is managed by the Authority for Digitalization of Romania (ADR). Through SEAP, the public institutions are electronically acquire whatever they need for their activities such as goods, services, ensuring in this way the transparency of the public funds spending process.

In order to electronically deploy the public acquisition procedures, the implementation norm for Law no. 98/2016 indicates that all the parties (the contracting authorities, the bidders and third parties associated with bidders) to apply the extended electronic signature based on a qualified certificate on the documents they upload on SEAP.

The contracting authorities should sign the documents uploaded on SEAP with this type of signature: the contracting strategy, the statement with the persons that have a decision making position, the assigning documentation, the additional clarifications/information attached to the assigning documentation, the requests for clarifications, the documents related to offer evaluations – the preliminary reports, the procedure report, the communications regarding the result of the procedure.

Furthermore, the bidders have the requirement to electronically sign all the documents uploaded on SEAP: the unique European procurement document (DUAE), the technical proposal, financial proposal, the answers to clarification requests, the qualification documents, etc. The electronic signature is an important element without this one the buyers do not have the right to initiate, in SEAP, the assignment procedures and the economic agents do not have the chance to win the contract assignment.

Although the utilization of electronic signature should not raise problems/questions, still, they have occurred in the assigning procedures on both the public entities and bidders, causing sometimes incidents such as expelling from bidding competition.

The most frequent problems had as an underlying cause the following:

- the extended electronic signature on the offer documents is no longer valid, the digital certificate being expired;
- the request to produce the original document although the one that has been loaded on SEAP contains an extended electronic signature;
- the technical/financial proposal were not signed with extended electronic signature;
- missing electronic signature from certain documents/ sections of the offer, although the offer, on the whole, has been signed;
- the extended electronic signature does not belong to the legal representative of the bidder;
- the documents coming from the subcontractors and/or their third parties associated with them do not have the same signature;
- the type of digital signature used by the bidders is not accepted;

a) Is the extended electronic signature assimilated with the handwritten (personal) signature?

Although the Law no. 455/2001 indicates that the document sent with such signature equates with the original ones, there are cases in which the members of evaluation commissions require to produce the original documents and in the case of nonconformity, the offer is rejected. In this situation, the removing from bidding competition is incorrect because the authenticity of the document has been ensured by loading the statement containing the electronic signature (NCSC a, 2021).

b) Does the missing the extended electronic signature leads to the offer rejection?

The implementation norms from Law no. 98/2016 (approved through Government Decision. no. 395/2016) explicitly state that the offer document should be signed with the extended electronic signature and not fulfilling this requirement is sanctioned with the rejection of the offer, according to article no. 137, paragraph (1), lit. j).

Loading the offer documents on SEAP and signing with a signature which does not have the specific elements of an electronic signature (name and surname of the signer, the date and the time of signing, the name of the digital certificate issuer, validity of the certificate) has caused the offer rejection due to missing extended signature (NCSC b, 2021).

c) Can the documents be signed with the extended electronic signatures, regardless of the file extension: pdf, p7m or p7s?

In an assignment procedure, the evaluation commission has considered as non-signed the offer with the extended electronic signature, based on a qualified certificate issued by a qualified provider, because the extension of the file that has included the signature was pdf.

However, relevant for the validation of an extended signature are those four elements mentioned by the Law no. 455/2001, at art.4, paragraph 4-5.

Regardless of the signature-associated file extension (".docx", ".pdf", ".p7S", "P.7M"), the signature should be considered if it has been used a valid qualified digital certificate issued by trust services provider.

If the commission members have doubts regarding the issuing of the signature by an accredited certification provider, they can contact ADR (NCSC c, 2020).

d) Technical issues that occurred during electronic signing should not automatically cause the offer rejection.

Following a clarification request for a technical proposal, the bidder has loaded on SEAP the document that has been requested by the evaluation commission however, during the application of electronic signature, a technical error has occurred. The offer has been rejected because the members of the commission have been unable to open the document with the attached electronic signature.

The offer rejection in such situation has been evaluated as not legal by the NCSC since the relevant information of buyer were available in other documents pertaining to the offer. The technical problem should have been evaluated as formal nonconformity (NCSC d, 2022).

e) Should the extended electronic signature be applied on each page of the document?

The rules established by the implementation norms of Acquisition Law requires the extended electronic signature of the offer and DUAE. Not following this rule causes the rejection of the offer in the case the offer and its attached document are not signed with extended electronic signature (EES) - art. 137 alin. (1) lit. j).

Although doesn't exist any requirement related to the application of EES on each page of the offer, quite often the evaluation commission has excluded the bidder from bidding competition due to missing EES on each page. One of the advantages of EES is the fact that, unlike the handwritten signature, there is no longer need that each page to be electronically signed. Through EES signing on the document, this is valid for all pages. Through a valid signature, it is confirmed that no changes have been made on the document. The technology that generates EES, encrypts the information and allows the detection of any changes applied to the document even if this will be on one or many pages. Therefore, an offer should not be rejected because the EES is not applied on all the pages of the electronic document.

Conclusions

The utilization of the electronic signature facilitates the conclusion of transactions, represents a solution to remotely stamp a document and to reduce the bureaucracy in public institutions and in business environment. The utilization of the advanced electronic signature based on a qualified digital certificate is equivalent to the handwritten signature of the document.

The deployment of the public acquisition transactions cannot be done without the utilization of the extended electronic signature on all the documents. The correct utilization of the electronic signature requires a training of the signers. ADR has an important role in the implementation of the digital signature in Romania.

The story of the digital signature is far from the end; it will develop and find new utilizations, and will be continue to be a strong and dependable tool, with direct applications in contracts (legal and economic aspects), but also in other matters, as for example demonstrating timeliness. It is very possible to find new utilizations for this tool.

The European Union has made possible the utilization of electronic signature across all EU Member States, achieving an important step toward a digital economy and society that is built on trust and security.

This paper can serve as a starting point for the next studies regarding the digitalization process, the access to online services or regarding the impact of the public policies on the digital transformation strategies for Romania.

References

1. *Directive 2014/24/EU of European Parliament and of the Council on public procurement and repealing Directive 2004/18/EC*. Official Journal of the European Union L 94.
2. European Union Agency for Network and Information Security, 2016. [online] Available at: <https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures/@@download/fullReport> [Accessed 27 May 2022].
3. European Commission, n.d. Trusted List Romania. *EU Trust Services Dashboard*, [online] Available at: <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/RO> [Accessed 28 May 2022].
4. Ministry of Finance, n.d. *Tax information and balance sheets* [online] Available at: <https://mfinante.gov.ro/persoane-juridice/informatii-fiscale-si-bilanturi > [Accessed 15 May 2022].
5. Farooq, S.M, Hussain, S.M.S., Ustun, T.S. 2019. Performance Evaluation and Analysis of IEC 62351-6 Probabilistic Signature Scheme for Securing GOOSE Messages. *IEEE Access*, vol. 7, pp. 32343-32351, 2019, [online] Available at: <doi: 10.1109/ACCESS.2019.2902571> [Accessed 20 May 2022].
6. *Government Decision no. 395/2016 for the approval of the secondary norms for the implementation of the provisions regarding the awarding of the public procurement contract/framework agreement as regulated by Law no. 98/2016 regarding public procurement.* Official Journal of Romania, no. 423 from June 6, 2016.
7. Kirillova, E. A., Bogdan, V. V., Lagutin, I. B., & Gorevoy, E. D. (2019). Legal status of smart contracts: features, role, significance. JURÍDICAS CUC, 15(1), pp. 285–300. [online] Available at: <https://doi.org/10.17981/juridcuc.15.1.2019.11> [Accessed 20 May 2022].
8. *Law no. 455 on July 18, 2001 on electronic signature*. Official Journal of Romania, no.429 of July 31, 2001.
9. *Law no. 98/2016 on public procurement*. Official Journal of Romania, no. 390/2016 of May 19, 2016.
10. Mandru, I., Saracu, A.F., 2021. Organization of Economic Activities in the Public Domain in the Post-Covid 19 Period. *Economics and Applied Informatics*, "Dunarea de Jos" University of Galati, Faculty of Economics and Business Administration, issue 3, pp. 94-98. [online] Available at: <doi: 10.35219/eai15840409228> [Accessed 15 May 2022].
11. Meshram, C., Lee, C., Meshram, S.G., Meshram, A. 2020. OOS-SSS: An Efficient Online/Offline Subtree-Based Short Signature Scheme Using Chebyshev Chaotic Maps for Wireless Sensor Network, in *IEEE Access*, vol. 8, pp. 80063-80073, 2020. [online] Available at: <doi: 10.1109/ACCESS.2020.2991348 > [Accessed 31 May 2022].
12. National Council for Solving Complaints, n.d. *Official Bulletin* [online] Available at: <http://portal.cnsc.ro/ >
    a) BO2021_610, Available at:
    <http://portal.cnsc.ro/buletinoficial.html?a=search&DPD:NumarBuletinSite=610#
    b) BO2021_2610 Available at:
    <http://portal.cnsc.ro/buletinoficial.html?a=search&DPD:NumarBuletinSite=2610&Dosar-CNSC:AnDosarString=2021#> [Accessed 31 May 2022].
    c) BO2020_1788, Available at:
    <http://portal.cnsc.ro/buletinoficial.html?a=search&DPD:NumarBuletinSite=1788&Dosar-CNSC:AnDosarString=2020#> [Accessed 31 May 2022];
    d) BO2022_902 Available at:
    <http://portal.cnsc.ro/buletinoficial.html?a=search&DPD:NumarBuletinSite=902&Dosar-CNSC:AnDosarString=2022#> [Accessed 31 May 2022].
13. *Order 449/2017, which modifies the implementation of 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 1999/93/EC*. Official Journal of Romania, no. 45 of June 20, 2017.

14. Pranckutė, R., 2021. Web of Science (WoS) and Scopus: The Titans of Bibliographic Information in Today's Academic World. *Publications*, 9(1), nr. articol 12. [online] Available at: <https://doi.org/10.3390/publications9010012> [Accessed 15 May 2022].
15. *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 1999/93/EC*. Official Journal of the European Union L 257, [online] Available at: <http://data.europa.eu/eli/reg/2014/910/oj> [Accessed 25 May 2022].
16. Ruica, E., Pura, M., Aciobanitei, I. Implementing Cloud Qualified Electronic Signatures for Documents using Available Cryptographic Libraries: A Survey, *2020 13th International Conference on Communications* (COMM), 2020, pp. 113-118, [online] Available at: <doi: 10.1109/COMM48946.2020.9141971> [Accessed 25 May 2022].
17. Suhail, S., Hussain, R., Khan, A., Hong, C.S., 2021. On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions. *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 1-17, 2021, [online] Available at: <doi: 10.1109/JIOT.2020.3013019> [Accessed 15 May 2022].
18. Vatra, N. Public Key Infrastructure for public administration in Romania. *2010 8th International Conference on Communications*, 2010, pp. 481-484, [online] Available at: <doi: 10.1109/ICCOMM.2010.5509037> [Accessed 25 May 2022].