ELECTRONIC DOCUMENTS AND TRUST SERVICES IN THE CONTEXT OF e-PROCUREMENT

This project has received funding from the European Union

2017

TABLE OF CONTENT

GLOSSARY

Directive 2014/24	Directive 2014/24/EU on public procurement and repealing Directive 2004/18/EC
Directive 2014/25	Directive 2014/25/EU on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC
Directive 2004/17	Directive 2004/17/EC coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors
Directive 2004/18	Directive 2004/18/EC on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts
Regulation 910/2014	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
Directive 1999/93	Directive 1999/93/EC on a Community framework for electronic signatures
PPA	Public Procurement Act
EDESA	Electronic Document and Electronic Signature Act
BES	Basic electronic signature
AES	Advanced electronic signature
QAS	Qualified electronic signature
TSP	Trust service provider
QTSP	Qualified trust service provider
BE Seal	Basic electronic seal
AE Seal	Advanced electronic seal
QE Seal	Qualified electronic seal
ICT	Information and communication technology
ESPD	European single procurement document
EC	European Commission

EU	European Union
eESPD	Electronic service on completing and submitting ESPD
e-Certis	Online repository of certificates (official documents)

LIST OF TABLES

1. BACKGROUND[i]

Setting electronic means of communication as the default manner in which information between contracting authorities (entities) and economic operators has to be exchanged throughout the public procurement process with the adoption of the 2014 directives (Directive 2014/24 и Directive 2014/25), is one of the most significant novelties, introduced by the European legislator in the public procurement realm. This approach may be defined as diametrically opposite to the rules on communication which were established by Directive 2004/17 and Directive 2004/18 according to which the use of electronic means of communication was only regarded as an option and not as a rule. The full transition to electronic means of communication (and transition to electronic procurement (e-Procurement) for that matter) is regarded by the legislator as allowing for a substantial simplification of the procurement process, an increase in its efficiency and transparency, as well as better participation opportunities for economic operators.

In 2014 another significant reform on Community level was also implemented – the adoption of the new Regulation 910/2014 which introduced an updated legal framework on the use and application of trust services. Alongside redefining the rules on the legal effect of electronic signatures, the regulation announced new types of trust services – electronic identification, electronic seal, electronic time stamp, certificate for website authentication, electronic registered delivery service; a new distinction between 'basic' trust service providers and 'qualified' trust service providers was defined; as well as new requirements towards ensuring and establishing effective cross-border interoperability and rules on recognition of qualified trust services and schemes between Member States.

With view of the above the matters related to the interrelation between the two legal areas have become particularly important, especially in terms of determining the level of applicability of trust services in e-Procurement context. In this sense when establishing the rules on electronic communication Directive 2014/24 and Directive 2014/25 refer to the provisions of the Directive 1999/93 and the related thereto subsidiary decisions of the European Commission[1]. Meanwhile the directive (as well as the commission implementation acts) was repealed and the rule that any references to the repealed directive are to be construed as references to Regulation 910/2014. Therefore a thorough assessment of the legal provisions affecting the possibilities, the necessities and the requirements on the application of trust services as part of the electronic procedures for the award of public contracts, is needed. This issue also exists on national level since the provisions of the 2014 public procurement directives were transposed without any significant alterations in the new Bulgarian Public Procurement act[2].

2. ELECTRONIC STATEMENT AND ELECTRONIC DOCUMENT

The legal certainty in civil and commercial matters is overshadowed by the existence of legal tools, which need to secure the exchange of those statements which are regarded by the law

[1] **2009/767/EC:** Commission Decision of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market; **2011/130/EU:** Commission Decision of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market .

[2] Promulgated SG, issue 13 of 16 February 2016, in force of 15 April 2016.

as the origin of legally important consequences – the constitution of rights and obligations. These tools in the modern world are the documents. Additionally - in order to secure the possibility for proving the authorship over documents, the law attaches significant importance to the handwritten signature.

Clarifying the nature of the electronic statement and the electronic document require an introductory analysis of the original notions related to 'document' and 'statement'. The established in the legal doctrine definition[3] in this sense reveals that a document is 'an object, an item, on which by means of writing or electronic symbols, a statement has been materialized'. Therefore any item can be considered a document, for as long as it contains a certain statement. The statement, on a separate note, can be viewed as the expression of the will of a legal entity, which is aimed at the achievement of a certain legally relevant result, while the document represents its material personification[4].

The electronic document (e-document) is defined by Regulation 910/2014 as 'any content stored in electronic form, in particular text or sound, visual or audiovisual recording'. As a result a significant difference between national and Community legislation exists – the Bulgarian EDESA recognizes as an e-document only the document in electronic form which contains a verbal statement. This is a result of the fact that the Bulgarian legislator defines the electronic statemen as a 'verbal (written with words) statement represented in digital form, through a commonly used standard for conversion, reading and visual representation of the information, which may contain non-verbal information'. On its turn the e-document is defined as 'an electronic statement stored on a magnetic, optical or any other type of carrier in a manner which allows for its reproduction'. It is clear that the European legislator gives the characteristics of an e-document to any content, regardless of whether it contains a verbal statement. This contradiction between national and Community law needs to be changed *de lege ferenda* in a manner through which compliance with the *acquis communautaire* is achieved. In fact, in this relation, the texts of the draft law amending and supplementing the EDESA[5], prepared under a legislative initiative serving this exact purpose, make it clear that it is very probable the future edition of the normative act will establish a provisional distinction between 'written (verbal) e-documents' and 'non-written (non-verbal) e-documents'[6].

In the above sense the electronic 'written' document is characterised on national level by a number of specific features, which distinguish it from the traditional hardcopy documents. As mentioned above, a peculiarity of this sort is the characteristic of the electronic statement of a **verbal statement** – written in words by the tools of written speech, understandable to people. Writing of any symbols or presentation of information in non-verbal form such as photographs, graphics, wingdings, etc., will not be considered both a verbal statement and document. The next characteristic of the e-document stipulates that the statement needs to be presented in **digital form,** which means representation and

[3] Stalev, Z. – 'Bulgarian Civil Proceedings Law', Ciela, Sofia, 2012, page. 273.

[4] Dimitrov, G. – 'Information and Communication Technology Law. Civil Law Aspects', Law and Internet Foundation, Sofia, 2014, page 60 et seq.

[5] See the proposed amendments of the provisions of Art. 2 and 3 with Draft Law on Amending and Supplementing the EDESA.

[6] Regardless of national law provision, with view of the direct effect of Regulation 910/2014, any contradiction which might exist has to be decided and interpreted in favour of the regulation.

conversion of the statement in ones and zeroes regardless of the applied technology. A further element from the notion for an electronic statement is the need for to be converted by the **use of a common, widely accepted standard,** allowing it to be perceived by the recipient[7]. The law envisages the possibility of an electronic statement containing **non-verbal information** in addition to the verbal one. Therefore if a legally relevant effect occurs as a result of the verbal statement being objectified and represented in digital form and through the use of a common and widely accepted standard, this representation would qualify as a legally valid electronic document.

With view of the provisions of Regulation 910/2014 a conclusion can be derived that it is no longer required for the electronic statement to be stored **on a magnetic, optical or any other carrier[8],** as well as it is no longer required for **the manner of storing of the statement, to allow for the statement's reproduction[9],** in order to be defined as a valid e-document**.** However it needs to be underlined that the lack of these two requirements does not change their practical application and importance. Simply storing (saving) cannot qualify the statement as an e-document. The possibility for reproduction remains a necessary requirement towards the validity of the e-document on a principle basis – the purpose of the document is to materialize the will of the author (the signatory) so that this will may reach to the consciousness of the recipient (the addressee). Without this being possible, the document loses its purpose and meaning. Therefore the impossibility for a reproduction of the content of the e-document in a manner which allows the addressee to perceive it, results in the document's de-validation.

Besides the above specifics, the following three basic characteristics of the e-document which relate to the e-document's legal effects, are of importance to the current work:

- Compared to the 'paper' hardcopy document which may exist in one original and many copies, the electronic document may exist in many originals. Each electronic copy is in fact an original. This peculiarity originates from the technological conditionality, where successful copying would not be possible unless every bit of information from the original is replicated, thus making distinguishing the copy from the original not possible. This characteristic of the e-document has a significant reflection on the manners used for gathering e-documents as evidence, where seizure or submission of an e-document is done through it being copied;
- The next important characteristic of the (written, verbal) e-document is that it is equivalised in terms of its legal effects to the written paper document by force of a legally fictional equation. Therefore whenever by the force of the law the written form is required as a condition for validity of certain statements, this requirement will be considered satisfied if a **'written'** e-document has been created. So a statement sent via e-mail, short text message, or in a social network, will be considered a written statement. Pursuant to art. 1, para. 2 of the EDESA the equivalisation does not cover

[7] These are such technological standards which are either recognised as such by a standardisation organisation, or have become standards through common use. The '.pdf' file format can be given as an example relating to the first hypothesis (created by the Adobe Corporation and recognised by the International Standardisation Organisation in the ISO 32000-1:2008 standard), while the '.doc' or '.docx' file formats created by Microsoft may be given as an example relating to the second hypothesis.

[8] See art. 3, para. 1 of the EDESA in relation to art. 3 para. 35 of Regulation 910/2014.

[9] The technology is not of relevance as long as the digitally stored data contain legally relevant statement.

those types of documents where 1) where the law requires a specific form of the document (the manner in which it is created) related to the validity of the statement contained thereto, or 2) the holding of the document is considered of legal importance on its own. Examples for the first group of exceptions can be given with the handwritten will, where the author handwriting the will has its own legal meaning, or the notary deed, where the special form for conducting the deal and the notary certification are of relevance. The second group of exceptions can include the bearer share, the promissory note, the cheque, etc.;

- Lastly, it should be noted that the unsigned e-document[10] can also be the cause of legal effects (results) in the same manner in which the signed one can. Of course the person benefiting from the document will have to prove who the author is, while the enforcement authority will have to evaluate its evidential weight in correlation with any and all other materials to the respective case.

3. DISTINCTION BETWEEN AUTHOR (SIGNATORY) AND RIGHT-HOLDER

According to the EDESA the 'author' of an electronic statement is the natural person who is claimed to be or pointed out by the statement as the person who made it. The next sentence of the provision at hand reveals that the 'right-holder' of the electronic statement is the person on whose behalf the statement has been made[11].

With view of the circumstance that the author of the electronic statement is the person who is **factually making it,** serves as a conclusion that only a natural person can be an author of an electronic statement. A legal person does not possess its own psychological activity and therefore cannot express will. The author of a document has to be distinguished from the person who has completed or drafted it – this person does not express will. In this sense if, for an example, the manager of a company tasks his secretary with drafting an e-document on his behalf – an internal order, the author of the document will be the manager and not the secretary. This can be easily illustrated through an additional example of drafting a document using the Microsoft Word application. As part of the metadata of a created text file, an 'author' field exists, which in fact represents predefined information on the user of the application, who may not in generally be considered, the author of the electronic statement, represented in the form of an e-document in the '.doc' or '.docx' file format. The accountant who has drafted the annual tax declaration is still not the author of the document – the author is the person who has signed it. The persons producing the documents only 'physically' prepare them. The person who is defined as an author in the statement itself will be considered as such and through his will the legal effects from the document will occur – in the above examples – the manager or the declarer.

[10] In this sense – Order No. 114 of 22.01.2014 on civil case No. 5892/2013 of the Supreme Court of Cassation; and Decision No. 70 of 19.02.2014 on civil case No. 868/2012 of the Supreme Court of Cassation.

[11] The distinction between 'author' or 'signatory' and right-holder exists only in national law and is not covered by Community legislation. Both Directive 1999/93 and Regulation 910/2014 refer only to the 'signatory' - a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents (within the meaning of Art. 2, item 3 of Directive 1999/93) and a natural person who creates an electronic signature (within the meaning of Art. 3, item 9 of Regulation 910/2014). It is very likely that this distinction will remain in the Bulgarian EDESA, regardless of the ongoing legislative initiative.

There can also be a difference between the person who has made the statement and the person whose behalf said statement has been made. In these cases the author forms the will and makes the statement, but does not enter into the legal relationships with third parties, as a result from the statement. Another legal entity – the right-holder will be bound by the legal effects, because the statement is being made on its behalf. The relationships between the author (signatory) and the right-holder may originate from a form of authorization or may be based on legal representation (a parent who is representing his child, a manager who is representing a company, a minister who is representing a body of state power, in relation to a public contract, etc.). As opposed to the 'author', the 'right-holder' can be a natural person as well as a legal person. It is precisely the right-holder who will acquire the rights and will assume obligations as a result of the statement. In other words – it is the legal status of the right-holder that will be affected by the legal effects.

4. ADDRESSEE OF THE ELECTRONIC STATEMENT (RELYING PARTY)

The function of documents and in particular – of e-documents – is for the will which they materialize to reach to the consciousness of the third persons to whom it is intended – the addressees of the statement. Pursuant to the EDESA, an addressee of an electronic statement 'is a person who **has been obliged by the force of the law[12] to receive electronic statements or for whom, through means of unequivocal circumstances, may be concluded, that has agreed to receive statements in electronic form'.** It is clear that through the cited provision the law establishes freedom in the use of the electronic form. As opposed to the 'paper' world, no one can be forced to receive electronic statements and thus be bound by their consequences, unless having previously consented to do so. This consent can be explicit or tacitly expressed, but its existence has to be assessed on the basis of '**unequivocal circumstances'**. This condition has its objective feature – the consent will be considered as existing whenever the behavior of the respective person, relevant facts and environment which accompany the receipt of the statement, does not do not give rise to suspicion and do not leave room for doubt, that the addressee has actually agreed to receive electronic statements.

5. HANDWRITTEN AND ELECTRONIC SIGNATURE

The handwritten signature may be defined as a graphic image (often done through writing the name of the author in full or in a stylised form), which allows determination of (1) the authorship of a specific statement, (2) the consent of the author with the statement, (3) the integrity of the statement, and (4) ensures the legal stability of the document with view of the legal results and proving the will of the author throughout time.

The development of information technologies and the possibility for an instantaneous exchange of electronic statements, without limitations in boundaries and, in practice for free, has led to the transfer of a significant amount of communication between people to occur in the electronic environment. Whereas the law associates certain legal consequences with some of these statements, the question of securing means to prove their authorship, as well as the rest of the functions of the handwritten signature – consent, integrity and non-repudiation, has become of significant relevance.

As a result of this question the concept of the electronic signature has been developed as an analogue to the handwritten signature in the virtual environment. The validity of this

[12] Currently this hypothesis relates only to bodies of state.

concept has been sanctioned in Bulgarian legislation by the EDESA. The law establishes three types of electronic signatures – basic, advances and qualified.

5.1. Basic Electronic Signature

The term 'basic electronic signature' is not explicitly defined neither in the EDESA, nor in Directive 1999/93 or the new Regulation № 910/2014. However the cited normative acts do contain a definition of 'electronic signature' which establishes the basis for the creation and functioning of the other two types of electronic signatures – the advanced and the qualified. For the purpose of clarity, this work uses the term 'basic electronic signature' because it represents a significantly simplified electronic signature form (format) when compared to the advanced and qualified types.

Pursuant to Regulation 910/2014 the basic electronic signature 'means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign'. It is made clear by this legal definition that **any data** in electronic form can be considered an electronic signature for as long it allows the addressee to unequivocally establish who the author (signatory) is. The prime condition is that said data is associated with the electronic statement in a specific manner – i.e. in a manner which allows determining the author[13].

Considering the multitude of technological solutions, the establishment of who the author is, can be done even automatically – e.g. based on the fact that the statement originates from a specific application which is under the sole control of the author (as a result the addressee trusts the claimed authorship) or due to the fact that the statement originates from a specific IP address, e-mail address or a mobile phone number. Meanwhile the technologically established and enforced certainty (the existence of which is required in terms of the other two types of signatures – advanced or qualified) on whether the author is precisely the person who has made the statement is irrelevant, from the perspective of the law. What matters here is whether the parties have agreed to consider the basic electronic signature as secure enough so that the functions inherent in each signature, can be considered as implemented – establishing the authorship, integrity, consent and non-repudiation. In this relation the EDESA stipulates[14], that in their relations, the parties may acknowledge the value of the basic electronic signature as equivalent to that of the handwritten signature[15]. This consent may be agreed upon as prior or subsequent to the electronic statement, it may also be explicit or tacit[16].

[13] Determining the author should be distinguished from identifying the author. Identification is a function traditionally associated with the advanced and qualified signatures and is not a requirement towards the basic electronic signature. It may be concluded that the term 'authorship' is used in a manner more closely related to the notion used for the purposes of intellectual property rights legislation and not so much as defining the personality. In practice the two notions are closely related and it is often not possible to distinguish them.

[14] See Art. 13, Para. 4, second proposition.

[15] Pursuant to Regulation 910/2014 only the qualified electronic signature is recognised as equivalent to the handwritten signature. The legal force of the other two types of signature is left to the national legislator to decide. This is precisely the idea behind the provision of Art. 13, Para 4 of the EDESA – providing the possibility for a contractual agreement between the parties based on which they might settle the legal force of the basic or the advanced electronic signature as equally binding to that of the handwritten signature.

[16] Whereas the legal provision uses the term 'consent' as well the plural 'parties', one may incorrectly conclude that a specific form for the manifestation of the will of the two parties is required. This is not the case – while the author addresses his statement to the other party, does that with the clear intent of being determined as

5.2. Advanced Electronic Signature (AES)

With respect to the AES Regulation 910/2014 sets a number of requirements in addition to those relating to the basic electronic signature.

Possibility to identify the author (signatory). The information in the form of an AES must allow identification of the signatory – i.e. the information must ensure the addressee that the statement originates from a specific person. As with basic electronic signature, this can be achieved through an automated system – e.g. through a unique user name and password of the signatory; an electronic device which generates one-time passwords, etc.; the goal of these methods is the same – a mean to authenticate (identification and access)[17].

Creation by the use of data under the sole control of the author (signatory). The requirement towards the AES creation manner requires an analysis of the notions 'electronic signature creation data' (electronic signature creation means) and 'control'. As regards to the 'electronic signature creation data' the legislative approach is neutral and does not point out to a specific technology. It is necessary that the respective technology allows the 'signing' in a manner which is under the sole control of the author. Therefore only the signatory must have control over the technology – i.e. access to the means through which the signature is created. The access may be physically and/or electronically secured[18].

Unique link to the author of the AES. Establishing a unique relation (link) to the author of respective data (by means of an AES) suggests the inability of another person to use the same information for identification. This signature method must ensure the addressee of the statement that it not originates from a specific person, but also that the statement cannot be issued by another, third person. Having in mind the example with the credit card – only the author knows the PIN code which allows access to the card. The card holder is the only person who has been made aware of it and only that person may use it. The PIN code links the device with the author in a unique manner.

Link to the data signed with the AES in a manner ensuring the detection of any subsequent changes. The fourth characteristic of the AES relates to methods which safeguard the content of the electronic statement. The link between the signatory and the statement must be ensured in manner which allows the detection of **any** subsequent changes in the statement as of the moment of its creation. This requirement guarantees the integrity of the statement. With the activation of the credit card in the respective card reader (POS terminal, ATM, etc.) the link presupposes the establishment of a secure communication session with the card operator and the bank. The statement cannot be changed thus ensuring the last requirement towards the AES.

---

the author. It would depend on the addressee whether to accept such a statement. So if the addressee responds to the statement it is clear that he has accepted the origin of the statement to be. Furthermore if from the actions of the addressee can be concluded that he accepts the claimed authorship, this might also be considered as consent (e.g. if the addressee, following the receipt of an offer in the form of an SMS for the purchase of a certain item, wires the remuneration directly to the offeror) which has been explicitly manifested.

[17] For example with credit cards – the bank identifies the cardholder through personalised procedure for identification prior to transferring it in his possession. Having in mind the requirement that only the cardholder holds and knows the means for identification and access (the plastic card and the associated therewith PIN code), the bank is ensured as to the identity of the person using the card.

[18] As in the above example with the credit card – the credit card is the mean giving access which is under the physical control of the cardholder. The cardholder is obliged not to handover the card to a third party.

As with the basic electronic signature, the EDESA allows contractual parties to acknowledge the value of the AES as equivalent to that of the handwritten signature.

5.3. Qualified Electronic Signature (QES)

Pursuant to the regulation the qualified electronic signature as an advanced electronic signature which complies with two additional requirements: (1) it is based on a qualified certificate for electronic signature issued by a trust service provider, which secures the link between the signatory and the public key, used for signature verification; and (2) is created by a qualified electronic signature creation device.

The main difference between the QES and the other types of electronic signatures originates from the legally established technological approach which needs to be used – the public key infrastructure. With this technology the verification of the authenticity of the electronic statement is done through the use of the so called 'public key' – this is one of a pair of keys. The other key (the private key) is used in the creation of the respective signature (the 'signing'). In its essence the private and public keys represent a pair of numbers. These numbers are not equal but are in a mathematical relationship with respect to the application of a specific algorithm for asymmetric encryption. In this sense each base pair is unique – i.e. only one public key corresponds to each private key. The private key is known only to the signatory while the public key may be known to third parties in order to establish the authenticity and integrity of the statement. The key pair however is in the possession of the author of the statement alone.

The general function of the qualified certificate is to establish sufficient legal security as to the relationship (the link) between the two keys in the base pair and the signatory. This is done by the issuance of the qualified certificate by a trust service provider.

The qualified certificate is specific electronic document which contains the name of the signatory, the public key which corresponds to the private key as well as a number of exhaustively listed attributes. This certificate is signed with the QES of the trust service provider and is attached to the electronic statement signed by the author. This ensures and establishes trust in the addresses that the public key from the qualified certificate is indeed in the possession of the signatory. In this way each third person may verify the truthfulness of the public keys of trust service providers, as they are legally required to publish their QES's certificates in a special publicly available register.

Therefore in prior to issuing the qualified certificate, the trust service provider must check the identity of the signatory; the fact that the private key is held only by the signatory as well as the fact that it (the private key) corresponds to the specific public key. The existence of a valid certificate is a precondition which allows accepting the validity of the QES.

A qualified electronic signature creation device (secure signature creation device) is the combination of hardware and software which is used for input of the data necessary for the creation of the QES. The use of such a device guarantees the validity of the QES. Its lack throughout the signature creation process de-validates the electronic signature as a qualified one. Secure signature creation devices must comply with the requirements set out in Appendix II to Regulation 910/2014.

With view of the above it may be summarized that the legal requirements towards QES aim at providing maximum electronic statement security – both in terms of authorship and integrity. In this sense the QES must be regarded as the electronic signature which is related

to the highest possible intensity of legally established guarantees. As opposing to the BES and the AES, the QES is acknowledged as equivalent to the handwritten signature by the force of the law (not based on a contractual agreement between signatory and addressee).

Table 1. Correlation between different types of signatures

№	Requirement	BES	AES	QES
1.	Data in electronic form	✓	✓	✓
2.	Establishing authorship	✓	✓	✓
3.	Possibility to identify the author (signatory)	-	✓	✓
4.	Unique link to the author (signatory)	-	✓	✓
5.	Unique data which is used by the author (signatory) to create an electronic signature	-	✓	✓
6.	Ensures the detection of any subsequent changes	-	✓	✓
7.	Qualified certificate for electronic signature issued by a QTSP	-	-	✓
8.	Created by the use of a secure signature device	-	-[19]	✓
9.	Acknowledged as equivalent to the handwritten signature	Contractually	Contractually	By the force of the law

6. OTHER TYPES OF TRUST SERVICES

Regulation 910/2014 introduces a number of other trust services alongside electronic signatures. These are:

- 'electronic identification' - the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person [20];

[19] It is possible to create an AES through means of a secure signature creation device. However the requirements towards these devices are different as if compared to the creation of a QES and are not so strict. They are not subject to Appendix II to Regulation 910/2014.

[20] Pursuant to the provisions of the Bulgarian Electronic Identification Act, the use of electronic identification is envisaged only for natural persons. The identification of legal persons in the electronic environment is done through their Unified Identification Numbers (UIC) issued in accordance with the Commercial Register Act or the BULSTAT Register Act.

- ‘electronic seal’ - data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity; the electronic seal can be basic, advanced or qualified;
- ‘electronic time stamp’ - data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time; electronic time stamp can be basic or qualified;
- ‘electronic registered delivery service’ - a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations; the electronic registered delivery service can be basic or qualified;
- ‘certificate for website authentication’ - an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued; the certificate for website authentication can be basic or qualified.

Table 2. Functions of the trust services

Service	Function
‘electronic identification’	Identification of a natural person in the electronic environment during remote data exchange. Cannot be used for the purpose of issuing statements but may be used as means of access to data for as long as a signature is not required;
‘electronic seal’	Guarantees the integrity of the data in electronic form as well as the correctness of the origin of that data (establishes authenticity). Serves as evidence that an electronic document was issued by a legal person, ensuring certainty of the document’s origin and integrity. Can be used only by a legal person (entity). In addition to data authenticity, the electronic seal an be used to authenticate any digital asset of the legal person, such as software code or servers;
‘electronic time stamp’	Establishes the moment of the creation of data in electronic form;
‘electronic registered delivery service’	provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations; the moment of sending and receiving is established by the means of a time stamp;
‘certificate for website authentication’	Establishes a process that enables the electronic identification of the origin and integrity of data in electronic form to be confirmed - a website; links the website to the natural or legal person (the owner of the website) to whom the certificate is issued.

The analysis of the content of different trust services shows a significant degree of similarity between electronic signatures and electronic seals which justifies comparing their functions and application.

Table 3. Comparison between electronic signatures and electronic seals

№	Requirement	BES	AES	QES	BE Seal	AE Seal	QE Seal
1.	Data in electronic form	✓	✓	✓	✓	✓	✓
2.	Establishing authorship (seal creation)	✓	✓	✓	✓	✓	✓
3.	Possibility to identify the author (signatory; creator of the seal)	-	✓	✓	-	✓	✓
4.	Unique data which is used by the author (signatory; creator of the seal) to create an electronic signature or electronic seal	-	✓	✓	-	✓	✓
5.	Unique means/data which is used by the author (signatory; creator of the seal) to create an electronic signature or electronic seal	-	✓	✓	-	✓	✓
6.	Ensures the detection of any subsequent changes	-	✓	✓	-	✓	✓
7.	Qualified certificate for electronic signature issued by a QTSP	-	-	✓	-	-	✓
8.	Created by the use of a secure signature device	-	-	✓	-	-	✓
9.	Acknowledged as equivalent to the handwritten signa-ture	Contractu-ally	Contractu-ally	By the force of the law	n/a	n/a	n/a

It is clear that both cases refer to a technological mean which ensures the origin and integrity (ensuring authenticity) of the data in electronic form. In this sense their application scope in terms of processed data is identical from the perspective of technological

requirements and purpose. The main differences between the electronic signature and the electronic seal are revealed in the following directions:

- While only a natural person can be the author, and both a natural and a legal person can be the right-holder of an electronic signature, with respect to the electronic seal – only a legal person can be its creator;
- There is a unidirectional interchangeability between the QES and the QE Seal – the use of QES by the legal representative of the legal person is equally acceptable to the use of a QE Seal. The opposite however is not possible;
- While national legislation allows parties to acknowledge the BES and AES as equivalent to the handwritten signature, there is no such possibility as regards the types of electronic seals[21].

7. ELECTRONIC PROCUREMENT (E-PROCUREMENT)

The mandatory use of electronic means of communication during the award of public contracts process is a significant step in the evolution of the public procurement regime. According to the 2014 directives, electronic means are defined as 'electronic equipment for the processing (including digital compression) and storage of data which is transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means'. Although the definition speaks of 'equipment' it may be concluded that the notion covers not only hardware but also the software resources, necessary for processing of information. In this sense, when defining the rules for communication, the legislation refers also to different tools and their characteristics. Therefore electronic documents and trust services will represent an important element of the data exchanged between contracting authorities (entities) and economic operators throughout the public procurement process.

The **general requirements** towards the implementation of e-Procurement in the context of the directives[22], can be listed as follows:

- Applied ICT solutions must be non-discriminatory, generally available and interoperable with the ICT products in general use; they must be in this sense directly accessible, without limitations;
- Applied ICT solutions must guarantee data security, integrity and confidentiality with respect to submitted requests to participate and tenders;
- Use of specific tools, devices or file formats which are not generally available or not or supported by generally available applications, is restricted;
- Providing possibility for use of specific file formats processed by generally available applications;
- Limiting the use of applications that are under a proprietary licensing scheme which can't be made available for downloading or remote use by the contracting authority;
- Use of specialized office equipment should be limited;

[21] This is understandable – Bulgarian legislation does not contain any requirement whatsoever relating to the mandatory use of a seal (stamp). From a legal perspective there isn't an object to refer to for the purposes of equivalisation.

[22] See Art. 22 of Directive 2014/24 and Art. 40 of Directive 2014/25.

- If however due to the characteristics of the public procurement the use of ICT solutions which are not in general use, is necessary, contracting authorities must provide the preconditions for the participation of all interested parties – to make such solutions available to potential tenderers and candidates by securing unrestricted, direct and free access by electronic means; or to provide different tools and devices through which required ICT solutions can be made available to economic operators.

If contracting authorities are not able to comply with the above requirements, the rules on electronic communication will not, as an exception, apply to them. In addition mandatory use of electronic communication will not apply in the cases of security breaches of the electronic means of communications or for the protection of particularly sensitive information (incl. classified information). In any case contracting authorities will have to justify and explain the reasons which lead to the use of non-electronic means of communication (conducting traditional public procurement).

In any case of e-Procurement contracting authorities will have to provide the following information to interested economic operators:

- Information on the characteristics and specifications necessary for electronic submission, incl. the cases where encryption and time-stamping will be applied;
- Information on the required security level for the electronic means of communication in the various stages of the specific procurement procedure;
- Information on trust services which will be applied throughout the e-procurement process.

The above information is also the subject of the requirement relating to providing unrestricted, free and direct full access.

The legally defined **specific requirements** towards electronic means of communication used in the e-Procurement process, are mainly related to the rules on providing access to submitted data:

- the exact time and date of the receipt of tenders, requests to participate and the submission of plans and projects can be determined precisely;
- ensuring that access to transmitted data is not made available prior the expiration of the respective time limits;
- only authorised persons may set or change the dates for opening data received;
- only for authorised persons may have access to all submitted data during the different stages of the procurement procedure;
- only authorised persons must give access to data transmitted and only after the prescribed date;
- data received and opened must remain accessible only to persons authorised to acquaint themselves with it;
- possibility to detect and register attempts for infringement of the accessibility rules and to detect and register any effective infringements.

The hereinabove resumed requirements of European legislation were transposed without any significant difference in the content of the Bulgarian PPA.[23] In addition, the Bulgarian legislator adopted a solution where a single national web-based platform (the platform) will be used for the purposes of e-Procurement[24], by all contracting authorities and entities[25]. The envisioned functionality of the platform covers all activities related to the award of public contracts, incl. contract implementation activities[26]. In this relation a significant number of the requirements on communication set forth by the directives should be viewed not as requirements towards individual contracting authorities, but as requirements towards the features of the future platform.

Table 4. Correlation between requirements towards individual contracting authorities and platform related requirements

Requirement	Contracting Authority	Platform
Applied ICT solutions related to submission of tenders or requests to participate must be non-discriminatory, generally available and interoperable with the ICT products in general use; they must be in this sense directly accessible, without limitations	-	✓
Applied ICT solutions must guarantee data security, integrity and confidentiality with respect to submitted requests to participate and tenders	-	✓
restricted use of specific tools, devices or file formats which are not generally available or not or supported by generally available applications	✓ (can be determined with respect to a specific public procurement, but in the general case is based on the features and functionalities of the platform)	✓ (can be determined with respect to a specific public procurement, but in the general case is based on the features and functionalities of the platform; as regards to public procurement documentation, compliance with the requirement will depend entirely on the platform's functionality)

[23] See Art. 39 – 40 of the PPA. Regarding the phased entry into force of PPA provisions on e-Procurement – refer to General Guide on the Public Procurement Legislative Environment in Bulgaria, OECD, 2016, page 91 et seq.

[24] The development, deployment and exploitation of the national e-procurement platform is yet to be implemented.

[25] Central purchasing bodies are allowed to operate their own solutions for the purposes of centralised procurement as long as technical interoperability and connectivity are established.

[26] Publication of procurement notices, decision and documents in the Public Procurement Register; Publication of Q&A with respect to a specific procedure; sending of invitations; submission of tenders and requests to participate; tender evaluation; signing of public contracts; ordering under a contract; e-invoicing; e-payments; exchange of other information and documents.

Requirement	Contracting Authority	Platform
providing possibility for use of specific file formats processed by generally available applications	✓ (can be determined with respect to a specific public procurement, but in the general case is based on the features and functionalities of the platform)	✓ (can be determined with respect to a specific public procurement, but in the general case is based on the features and functionalities of the platform; as regards to public procurement documentation, compliance with the requirement will depend entirely on the platform's functionality)
limiting the use of applications that are under a proprietary licensing scheme which can't be made available for downloading or remote use by the contracting authority;	✓ (can be determined with respect to a specific public procurement, but in the general case is based on the features and functionalities of the platform)	✓ (can be determined with respect to a specific public procurement, but in the general case is based on the features and functionalities of the platform; as regards to public procurement documentation, compliance with the requirement will depend entirely on the platform's functionality)
Use of specialized office equipment should be limited	-	✓
Securing unrestricted, direct and free access by electronic means to ICT solutions which are not in general use; or providing different tools and devices through which required ICT solutions can be made available to economic operators	✓	-
Providing information on the characteristics and specifications necessary for electronic submission, incl. the cases where encryption and time-stamping will be applied	-	✓
Determining the security level for the electronic means of communication in the various stages of the specific procurement procedure	✓	-
Trust services which will be applied throughout the e-procurement process	✓ (can be determined with respect to a specific public procurement, but in the general case is based on the features and functionalities of	✓ (can be determined with respect to a specific public procurement, but in the general case is based on the features and functionalities of the platform; the platform has to

Requirement	Contracting Authority	Platform
	the platform)	ensure the use of all types of trust services applicable with respect to e-procurement – QES and QE Seal as a minimum)
the exact time and date of the receipt of tenders, requests to participate and the submission of plans and projects can be determined precisely	-	✓
ensuring that access to transmitted data is not made available prior the expiration of the respective time limits only authorised persons may set or change the dates for opening data received	-	✓
only for authorised persons may have access to all submitted data during the different stages of the procurement procedure	-	✓
only authorised persons must give access to data transmitted and only after the prescribed date	-	✓
data received and opened must remain accessible only to persons authorised to acquaint themselves with it	-	✓
possibility to detect and register attempts for infringement of the accessibility rules and to detect and register any effective infringements	-	✓

The content of the 2014 directives, Regulation 910/2014 and the national law show that trust services which have to be included as functionalities of the future platform, refer to electronic signatures and the qualified electronic seal as a minimum (possibly electronic identification too, depending on whether the platform would allow accessing data on the basis of user identification/authentication, but which does not lead to an electronic statement – i.e. signing of an e-document). This conclusion is based on the understanding that under the provisions of Regulation 910/2014, contracting authorities will not be able to decide on whether to accept or not e-documents submitted by tenderers or candidates which are signed with a QES or sealed with a QE Seal, as long as the verification and validation processes are successful and regardless of whether the use of such has been required for the purposes of the procedure. In this sense the PPA stipulates that whenever a tenderer or a candidate uses different format of electronic signature, the electronic signature or the electronic document carrier has to include information on existing

validation possibilities[27]. This requirement does not apply in the cases where the tenderer or candidate has used an electronic signature (AES based on a qualified certificate or QES), which has been issued by a QTSP, that is included in the respective trust list[28].

In needs to be noted that legislation allows contracting authorities to determine the format of applicable electronic signatures (and hence – the applicable electronic signature type – BES, AES, AES based on a qualified certificate or QES). When doing so contracting authorities must take into account the necessary security level associated with the electronic means of communication throughout the different procurement stages, which has to be proportional to risks attached[29]. Contracting authorities may determine different electronic signature formats for the different stages of the award of contract procedure. Therefore the platform must ensure the respective functionality allowing the application of each of the above electronic signature types.

Table 5. Applicability of different types of signatures

	Contracting Authority	Tenderer / Candidate
Application of BES	**Applicable under condition** The contracting authority may apply BES for the purposes of communication with tenderers or candidates, if such possibility has been envisaged (and on the basis of the functionalities of the platform), and under the condition that the respective tenderer or candidate has agreed to that. The contracting authority will be required to provide information on the specifications applicable to the BES throughout the submission process[30] (accordingly – to point out applicable platform functionality). The contracting authority must ensure unrestricted, free and direct full access by electronic means to the tools and devices the means for signature creation, or to other tools and devices, through which the means for BES creation can be accessed/created by the interested parties	**Applicable under condition** The tenderer or candidate may use BES: if the contracting authority has allowed this option, in accordance to the security level determination for the specific procedure and with view of the electronic means to be used; in accordance with the BES creation means and functionalities of the e-Procurement platform

[27] Online, for free and in a manner which is understandable to the persons to whom the language is foreign.

[28] See Art. 22 of Regulation 910/2014.

[29] Drafting and issuing methodological guides may be considered a good recommendation in this relation. Determining the risk levels may include: the risk to the proper functioning and integrity of the specific procurement process; risks to national security or risks associated with the handling of sensitive or classified information; the risk of inadvertent or unauthorised disclosure of, or access to, any economic operator's confidential information; he risk of inadvertent or unauthorised disclosure of, or access to, information held by the contracting authority including information relating to the specific procurement; the risk that use of electronic communications could provide opportunity for malicious attacks on the electronic systems of, or data held by, the authority, any economic operator or any other person, including introduction of malware or denial of service attacks; other material risks relating to the procurement procedure in question, etc. It is clear that a significant portion of the above risks and mitigation measures will have to be dealt with on the level of the centralised platform.

[30] Based on Art. 13, Para. 4 of EDESA, in relation to recital 49 of Regulation 910/2014.

	Contracting Authority	Tenderer / Candidate
	(if the use of such is required).	
Application of AES	**Applicable under condition** The contracting authority may apply AES for the purposes of communication with tenderers or candidates, if such possibility has been envisaged (and on the basis of the functionalities of the platform), and under the condition that the respective tenderer or candidate has agreed to that. The contracting authority will be required to provide information on the specifications applicable to the AES throughout the submission process, including where encryption and time stamping is needed (accordingly – to point out applicable platform functionality). The contracting authority must ensure unrestricted, free and direct full access by electronic means to the tools and devices the means for signature creation, or to other tools and devices, through which the means for AES creation can be accessed/created by the interested parties.	**Applicable under condition** The tenderer or candidate may use AES: if the contracting authority has allowed this option, in accordance to the security level determination for the specific procedure and with view of the electronic means to be used; in accordance with the AES creation means and functionalities of the e-Procurement platform. In the general case, due to technical and technological reasons related to AES interoperability, the use of an AES which has not been created by the means of the platform and/or has not been intended for use within the platform, would not be possible. Regardless of that if the tenderer or candidate uses an AES, different from the one determined by the contracting authority, but which may function within the platform, said tenderer or candidate will be obliged by the force of the law to provide information on signature validation means.
Application of AES, based on qualified certificate[31]	**Applicable under condition** The contracting authority may apply AES, based on qualified certificate for the purposes of communication with tenderers or candidates, if such possibility has been envisaged (and on the basis of the functionalities of the platform), and under the condition that the respective tenderer or candidate has agreed to that. The contracting authority will be required to provide information on the specifications applicable to the AES, based on qualified certificate, throughout the submission process, including where encryption and time stamping is needed (accordingly – to point out applicable platform functionality). The contracting authority must ensure unrestricted, free and direct full access by electronic means to the tools and devices	**Applicable under condition** The tenderer or candidate may use AES, based on qualified certificate: if the contracting authority has allowed this option, in accordance to the security level determination for the specific procedure and with view of the electronic means to be used; in accordance with the AES creation means and functionalities of the e-Procurement platform. In the general case, due to technical and technological reasons related to AES interoperability, the use of an AES, based on qualified certificate, which has not been created by the means of the platform and/or has not been intended for use within the platform, would not be possible. Regardless of that if the tenderer or candidate uses an AES, based on qualified certificate with a format different from the

[31] Up until the adoption and the entry into force of Regulation 910/2014 the AES, based on qualified certificate has been unknown to Bulgarian legal system. It still remains unsettled on national level while EU legislation does not contain a proper definition. AES, based on qualified certificate may be defined as a subtype of AES, or as an intermediate level between AES and QES. The main difference between AES and QES is that the requirements for the use of a (secure) qualified electronic signature creation device does not apply in the case of AES creation.

	Contracting Authority	Tenderer / Candidate
	the means for signature creation, or to other tools and devices, through which the means for AES, based on qualified certificate, creation can be accessed/created by the interested parties.	one determined by the contracting authority, but which may function within the platform, said tenderer or candidate will be obliged by the force of the law to provide information on signature validation means, regardless of the signature having been issued by a QTSP.
Application of QES	**Always applicable**	**Always applicable**

A matter which needs to be decided when specifying the requirements towards the functional and non-functional parameters of the platform, is the question relating to the application of other kinds of trust services, as well as determining their type (qualified or non-qualified (basic). In this sense the requirement for a precise determination of the exact time and date of the receipt of tenders, requests to participate, would imply the application of a time stamp, respectively – qualified time stamp. Additionally the requirement towards achieving a significant level of security (both technical and legal) in the communication between contracting authorities and economic operators may justify the application of the registered electronic delivery service, respectively – the qualified registered electronic delivery. As long as there are no specific requirements in that direction, an approach can be adopted where the functionalities associated with the above two trust services is implemented as part of the platform itself without the use a TSP or a QTSP.

8. APPLICATION OF THE ESPD IN THE E-PROCUREMENT FRAMEWORK

The ESPD is defined as a self-declaration of the businesses' financial status, abilities and suitability for participation in the award of public contract procedure. With the implementation of the possibility for an ESPD submission tenderers and candidates are no longer required to provide evidence for their compliance with the personal standing and qualification requirements of contracting authorities. The content of the ESPD was introduced by the adoption of Implementing Regulation 2016/7 of the EU Commission on establishing the standard form for the European Single Procurement Document. Pursuant to the provisions of the EU directives the use of the ESPD as an electronic document will become mandatory as of 1 April 2018.

Currently the EC provides a free electronic service with limited functionalities which may be of use to participants in the public procurement process, who may want to electronically prepare an ESPD (eESPD)[32]. The form may be completed online, may be printed and may be used in a specific procurement procedure. As for e-Procurement, current functionality allows ESPD downloading and saving for the purposes of electronic submission[33].

Besides establishing the standard form of the ESPD and the above web-based service of the EC, the following additional tools are currently being developed:

- ESPD Exchange Data Model (EDM), which facilitates the eESPD integration with the existing national e-Procurement solutions, incl. - pre-qualification services[34];

[32] The service is available here: https://ec.europa.eu/tools/espd/filter?lang=en

[33] Through the e-Delivery infrastructure which will be developed under the e-SENS project (www.esens.eu).

[34] Available here: https://github.com/ESPD/ESPD-EDM

- Open source eESPD version, compatible with the data exchange model, allowing customization of specific functionalities in relation to national law requirements[35];
- Virtual Company Dossier, which allows automated data processing[36]; and
- The ESPD/VCD Designer which is a standalone web application which provides a full range of ESPD and VCD functionalities to the economic operators and the contracting authorities (such as initial creation of criteria, requirement groups and requirements for the ESPD Request or VCD Request for contracting authorities; functionalities related to the fulfilment of such requirements for economic operators; and validation of completed documents functionality both for economic operators and contracting authorities)[37].

The above listed resources are directed towards future implementation by contracting authorities and economic operators, of:

- Initial drafting and subsequent multiple use of an already completed ESPD (one time creation – multiple usage);
- The possibility to directly input specific requirements, for a specific tender and evidencing documents, without the need of a separate reference in e-Certis;
- The possibility for an automated check on the compliance of the interested person with the pre-qualification requirements prior to tender or request to participate submission;
- The possibility for an automated check by the contracting authority for the compliance of a tenderer or a candidate with the pre-qualification requirements following the submission of a tender or request to participate during the prequalification stage of a procurement procedure;
- Facilitating communication between economic operators with respect to joint tendering in public procurement procedure;
- The possibility for ESPD information summarization by contracting authorities during a tender procedure;
- Integration of eESPD with e-Certis.

9. E-CERTIS AS A REFENCE TOOL AND ONLINE RESOURCE

The e-Certis (an online repository of certificates) is a reference tool which allows the identification and comparison between different official documents (certificates) which might be used for the purposes of public procurement throughout the EU.

Prior to the adoption of the 2014 directives, e-Certis was kept up to date and was verified by national authorities on a voluntary basis. According to the new legislation the pursued objectives through the implementation of e-Certis are related to strengthening cross-border procurement. In this relation in terms of e-Certis service implementation contracting

[35] Available here: https://joinup.ec.europa.eu/asset/espd/home

[36] Further information is available here: https://www.esens.eu/content/e-sens-sample-software-implementation-european-single-procurement-document-available

[37] The application is available here: https://joinup.ec.europa.eu/catalogue/asset_release/vcd-virtual-company-dossier

authorities will be encouraged to require primarily such types of certificates or forms of documentary evidence that are covered by e-Certis, for the purposes of establishing compliance by economic operators with the pre-qualification criteria set out for a specific public procurement.

The current voluntary approach on keeping e-Certis data up to date will be replaced by the process of compulsory updating of the certificates' related information by Member States. National pre-qualification databases (registers; aggregators; other pre-qualification services), containing relevant information on economic operators will be linked through e-Certis[38], which will allow automated and one-time input of information as well as automated assessment of tenderers' and candidates' compliance with prequalification criteria. Competent national authorities will be obliged, upon a specific request, to provide other Member States any information related to such databases which may be used for references on ESPD contained and self-declared circumstances regarding economic operators[39].

[i] This Policy Paper was developed and written by Boyan Ivanov and Radina Tomanova on behalf of *Dimitrov, Petrov & Co* under the direction of Paulo Magina, Head of the OECD Public Procurement Unit and Petur Berg Matthiasson, Policy Research and Advice, OECD Public Procurement Unit with contribution from Zdravka Pekova, Local Coordinator for the OECD in Bulgaria for this project.

[38] Currently the information system which will provide the entire scope of e-Certis functionalities is still being developed and is not operational. In this regard and with view of the brief nature of legal provisions, it is not possible to provide a thorough assessment on the full capabilities of the online repository and means of use.

[39] In the Bulgarian context these will include the commercial register; the BULSTAT register; professional registers such as the Bulgarian BAR Registers operated by the Supreme Bar Council, the Central Professional Register of Constructors operated by the Bulgarian Constructors Chamber, etc.