CONTENT

Definitions

Directive 95/46/EO	Directive 95/46/EC of the European Parliament and of the Council of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
EDETSA	Electronic Document and Electronic Trust Services Act, promulgated in SG, no. 34 of 06.04.2001, as amended and supplemented upon the adoption of these General Terms and Conditions.
Qualified Electronic Signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
Qualified Trust Service	A certification service that meets the applicable requirements set out in Regulation (EU) No 910/2014. An individual who creates an electronic signature. Data in electronic form that is added to, or logically associated with, other data in electronic form and which the holder of the electronic signature uses to sign.
Supervisory Body	
Regulation (EU) № 910/2014	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
SEP Bulgaria	"System for Electronic Payment Bulgaria / SEP Bulgaria" JSC, a joint stock company registered under Bulgarian law, with UIC 131107204
Trust Service	An electronic service provided by SEP Bulgaria for remuneration consisting of: (a) the creation and verification of electronic signatures, electronic seals and electronic time stamps as well certificates relating to these services;
Advanced electronic signature	An electronic signature that meets the following requirements: (a) linked in a unique way to the signature holder; (b) be able to identify the signature holder;

	(c) created through data to create an electronic signature that the holder of the electronic signature can uses with a high degree of trust and only under his own control; and (d) associated with the data that has been signed with it in such a way as to permit any subsequent change to be made.
CPS	Practice in providing qualified trust services
CRL	List of suspended and terminated certificates

1. General

"Electronic Payment System Bulgaria / SEP Bulgaria" JSC (SPS) is an accredited Trust Services Provider (TSP) pursuant to Article 19 of the EDETSA and Art. 3, item 19 of Regulation (EC) No 910/2014, promulgated in the State Gazette no. 100/2010 these Terms and Conditions (General Terms and Conditions) combine "SEP Bulgaria's Practice in Trust Services" (here and hereinafter referred to as "Practice") and "Trust Policy" of SEP Bulgaria (here and hereinafter referred to as "Policy"), and details the rules regarding the Trust Practice of SEP Bulgaria, as well as describes the processes of certification services delivery and the scope of application of the electronic signature certificates resulting from these services.

The practices of providing qualified certification services of SEP Bulgaria are reviewed in summary in this section.

1.1. Qualified Trust Services Provider

SEP is a qualified trust services provider and provides these services in accordance with the applicable legislation through a certification authority and a system of registration bodies. The certification authority and the registration bodies perform their activities on the provision of qualified trust services in the name and on behalf of SEP Bulgaria.

The certification authority issues qualified trust electronic signature certificates (QTESC) to individuals and individuals associated with legal entities as well as qualified certificates for qualified electronic seal (QCQES) to legal entities and qualified electronic time stamps (QETS). The certifying authority carries out activities that involve issuing, renewing, suspending and resuming, terminating qualified certificates, keeping a register and providing access to it.

Registration authorities

SEP Bulgaria provides its services through a system of registration authorities. The registration bodies have the following functions: (i) checking the requests for the issuance of the QTESC and the QESC, (ii) identifying and verifying the subscribers, (iii) acting after approval of the requests and issuing of the certificates, (iv) renewal, termination , suspension and renewal of certificates.

The registration bodies act on behalf of SEP Bulgaria, in accordance with its policies, practices and procedures. RB accepts, verifies and approves or rejects requests for issuance, modification, renewal, suspension / resumption and termination of qualified electronic signatures / seals certificates. When checking the identity or identity of the holder / creator, the RB's operators directly or indirectly identify the persons to whom qualified certificates will be issued using identification methods giving the same degree of security as physical identification. SEP Bulgaria concludes a contract with the RB (in the cases when the specific RB is a unit outside the legal organization of SEP Bulgaria), by virtue of which the activities described above are carried out, as the Practice and the Policies of the Provider are part of this

contract. Any person may act as the Provider's RB after having stated this and fulfilling the conditions arising from SEP Bulgaria's Regulatory Documents. The list of RBs that are authorized by SEP Bulgaria is public and is available on the SEP Bulgaria website.

It Is forbidden that qualified certificates of SEP Bulgaria are used in a manner incompatible with the stated purpose. Certificates issued and provided to users by SEP Bulgaria can be used to:

- Establishing identity and identity of a natural person or a natural person associated with a legal person in his or her legal or contractual capacity;
- Evidence that an electronic document or other information object has been issued by a legal entity ensuring the reliable origin and integrity of the document, respectively the information object, by means of an electronic seal, accompanied by a qualified certificate for electronic printing issued by the SEP Bulgaria;
- Signing, encryption and decryption of electronic data, such as electronic documents, databases, information objects, e-mail, and others;
- Checking signed data, such as documents, recommended e-mail, and others;
- Encryption and decryption of data and exchange of keys used for encryption;
- Information on the applications that can use the qualified certificates issued by SEP is published on the Internet site of the Provider [https://www.esign.bg/bg/services/public-register/].

1.2. Holder

The electronic signature holder is the individual who creates the electronic signature. A Holder may also be a natural person who is associated with a legal entity to sign electronic statements in accordance with his representative authority. The qualified certificate shall also indicate the person representing the Holder. The electronic signature holder may entrust the servicing of the equipment for creation of to a third party, provided that appropriate mechanisms and procedures are in place to ensure that the Holder has sole control over the use of the data associated with the creation of his electronic signature Only the qualified certificate Holder has the right to access the private key for signing electronic statements through which he creates an advanced or qualified electronic signature.

1.3. Relying party

A Relying party means a natural or legal person who relies on a certification service. In essence, the Relying party receives documents signed with an electronic signature / seal by taking action, trusting in the qualified certificate for the relevant electronic signature / seal. The Relying party is responsible for verifying the validity of the qualified electronic signature / seal certificate. Relying parties shall assess whether the type of qualified electronic signature / seal certificate and the guarantees associated with

it are sufficient for the purposes for which it is used. Relying parties should have knowledge and skills on the use of qualified certificates, especially as regards the level of security in checking the identity of the Holder and the identity of the Issuers of these qualified certificates, as well as the applicable restrictions on their use. Relying parties have permanent access to SEP Bulgaria's registers for checking the validity of qualified certificates, establishing the electronic identity of the Holder /Issuer, or other circumstances and data reflected in the certificates or entered in these registers. Trustworthy countries established outside the territory of the Republic of Bulgaria can rely on reliable, secure, easy and convenient qualified automated validation of qualified electronic signatures / stamps issued by SEP.

1.4. Seal creator

The print creator is a legal entity that creates an electronic seal. The creator performs on its own, electronic statements, which electronically stamp in accordance with its representative power. The creator is listed in the qualified electronic print certificate as an Issuer. Only the Issuer as a qualified certified user has the right to access the private key to stamp electronic statements through which he creates an advanced or qualified electronic seal.

2. Services Provided

2.1. Qualified certificate for a qualified electronic signature

A qualifyed certificate for a qualified electronic signature enables an individual (an electronic signature holder) participating in an electronic transaction to identify itself to other participants in that transaction.

QTESC contain:

- indication that the certificate was issued as a qualified certificate for qualified electronic signature;
- a dataset that uniquely represents the qualified trust service provider that has issued the qualified certificate and:
  - with respect to a legal entity: name and UIC,
  - with respect to an individual: name of the person;
- the name of the holder;
- electronic signature validation data that corresponds to the electronic's signature creation data;
- information on the beginning and end of the validity period of the certificate;
- certificate identification code unique to SEP;

- advanced electronic signature or SEP's advanced electronic seal;
- where the certificate that maintains the advanced electronic signature or advanced electronic seal is available free of charge;
- the place of services to which requests for verification of the validity of the qualified certificates are to be addressed;
- in cases when the data for issuing of an electronic signature associated with the electronic signature validation data is located in a device for creating a qualified electronic signature, this is indicated at least in a form suitable for automated processing.

QTESC issued to natural persons:

QTESC are issued to individuals (electronic signature holders) and can be used to identify the subscriber, protected and encrypted sending of electronic messages and secure and encrypted communications, access to information and online internet transactions of all kinds. Ensure a high level of identity requiring the applicant to prove his identity by appearing personally or through a representative duly empowered by a notarized power of attorney before a registration body. The validity of these QTESC is defined in the qualified trust services agreement.

QTESC issued to natural persons associated with legal entities:

QTESC are issued to natural persons (holders of electronic signature) who are associated with legal entities. They can be used to identify the subscriber, protect and encrypt emails and secure and encrypted communications, access to information and online internet transactions of all kinds. Ensure a high level of identity requiring the applicant to prove his identity by appearing personally or through a representative duly empowered by a notarized power of attorney before a Registration Authority. The validity of these QTESC is defined in the qualified trust services agreement.

2.2. Qualified certificate for qualified electronic seal

A qualified certificate for a qualified electronic seal enables a legal entity participating in an electronic transaction to identify itself with the other participants in that transaction by linking the electronic seal validation data to the legal entity and confirming that person's name.

QCQES contain:

- indication that the certificate was issued as a qualified certificate for qualified electronic seal;
- a dataset that uniquely represents the qualified trust service provider that has issued the qualified certificate and:

- with respect to a legal person: name and UIC,

- at least the name of the print maker and, if applicable, the UIC;
- electronic seal validation data that matches the data for creation of the electronic seal;
- information on the beginning and end of the validity period of the certificate;
- certificate identification code unique to the SEP;
- advanced electronic signature or SEP advanced electronic seal;
- where the certificate that maintains the advanced electronic signature or advanced electronic seal is available free of charge;
- the place of services to which requests for verification of the validity of the qualified certificates are to be addressed;
- in cases when the data for issuing of an electronic signature associated with the electronic signature validation data is located in a device for creating a qualified electronic signature, this is indicated at least in a form suitable for automated processing.

QCQES are issued to legal entities (issuers of qualified electronic seal). They can be used to identify the subscriber/ creator of qualified electronic printing, protected and encrypted sending of electronic messages and secure and encrypted communications, access to information and online Internet transactions of all kinds. Ensure a high level of identity requiring the applicant to prove his identity by appearing personally or through a representative duly empowered by a notarized power of attorney before a registration body. The validity of these QCQES is defined in the qualified trust services agreement.

2.3. Qualified electronic time stamp

The qualified electronic time stamp makes it possible to establish that data in electronic form that binds other data in electronic form at a particular point in time, that the latest data existed at the time and is proof of it. Qualified electronic time stamping is based on the presumption of accuracy of the date and time indicated by it, and for the integrity of the data with which the date and time are bound.

3. Technology for using QTESC / QCQES

This section discusses the technology of obtaining, installing and using qualified electronic signature certificates and qualified electronic seal certificates. Qualified certificates are issued by SEP on a smart card.

3.1. Preliminary preparation

The preparation process for obtaining and installing a qualified certificate and using the electronic signature / electronic seal includes the following basic steps:

- Submission of a qualified certificate request;
- Checking the identity of the applicant;
- Issuance of a qualified certificate from the SPS;
- Get the Qualified Certificate and Smart Card Access Details;
- Install the qualified SER certificate of the subscriber's hardware;
- Providing conditions for protection of the private key and the qualified certificate;
- Selection and installation of application software for use of the private key and the qualified certificate;

3.2. Signing / issuing of a seal

Signing with an electronic signature / issuing of a seal is done by using the application software for use of the private key.

The electronic signature holder / seal issuer must strictly follow the instructions given by the developer of the application software and comply with the restrictions and conditions of use set forth in the regulatory framework, this document, Practice in providing qualified trust services and the Policy for providing qualified certificates.

3.3. Identification

Qualified certificates for qualified electronic signature / electronic seal issued by SEP Bulgaria can be used to identify the subscriber to remote web server access in the following way:

- through using the subscriber's browser, the location that is the object of remote access (usually the URL) is selected;
- when making the connection to the server, the subscriber is required to select and confirm the appropriate QTESC / QCQES that he/ she will use to gain access to the remote resources;
- after successfully completing the identification session, the subscriber gets access to the remote resources, in accordance with the rights granted to him/ her.

4. Verification of electronic signature / electronic seal

The purpose of the electronic signature / electronic seal check is to establish that:

- the electronic signature / electronic seal was created with a private key that corresponds to the public key entered in the qualified certificate of the electronic signature holder/ seal issuer;
- the message/ electronic document was not changed after the electronic signature/ electronic seal was created.

Upon receipt of a signed electronic statement / electronic document confirmed by an electronic seal, the addressee (the relying party) must, before deciding whether to trust this electronic signature / electronic seal, perform at least the following actions:

- Understand the principles and rules of ESign for issuing and managing qualified certificates;
- Check (using the application software) the state of the electronic signature / electronic seal - whether the electronic statement / electronic document has been changed after the electronic signature / electronic seal has been created;
- Check the period of validity entered in the qualified certificate of the electronic signature holder / seal issuer;
- Download from website of SEP Bulgaria the latest copy of the publicly available List of suspended or discontinued certificates (CRL);
- Install the CRL and update the suspended and discontinued certificates database on the local computer being audited;
- Visually or automatically (via the application software) check the status of the qualified certificate whether the qualified certificate of the electronic signature holder/ seal issuer of the received electronic statement / electronic document is included in the current CRL.

Following these steps, if it deems necessary, the addressee may also take other lawful actions for further scrutiny before taking the final decision on whether to trust the electronic signature / electronic seal and the qualified certificate. In any case, the addressee must trust the electronic signature / electronic seal and the qualified certificate only to the extent reasonably reasonable for the circumstances.

5. Technology for Using Qualified Electronic Time Stamps (QETS)

Verification of the date and time of submission of an electronic document shall be made in accordance with IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) after the subscriber submits an electronic request to a SEP address specified by SEP Bulgaria. The request is submitted to SEP as a certification service provider and it performs the time verification activities.

6. Requirements for private key storage

The private key of the asymmetric cryptographic system must be stored in a highly secure environment. This section discusses the essential requirements for the storage of the private key of the electronic signature holder / seal issuer/ person.

6.1. Physical storage

After generating the key pair on the smart card and providing the activation data for the smart card to the subscriber, the responsibility for the physical protection of the private key is entirely borne by him, respectively, by the electronic signature / seal issuer.

The subscriber, respectively the electronic signature holder/ seal issuer, must take appropriate measures to prevent unauthorized physical access to the medium (the smart card) containing the private key. Only the electronic signature holder (print creator) should be able to access the medium, which will protect the private key and the qualified certificate from unauthorized access or use of the electronic signature / electronic seal by another person other than the holder to whom it was issued.

6.2. Export

When the private key is stored on a smart card, it cannot be exported, but the electronic signature / seal issuer must not give others the ability to access the smart card containing the qualified certificate.

6.3. Operational storage of the private key

In case of operational work, when the smart card on which the private key and the qualified certificate are not used temporarily, they should not be left unattended in a publicly available location. Failure to comply with this requirement creates preconditions for compromising the private key of the subscriber.

6.4. Personal identification number (PIN)

The access to the private key and the qualified certificate provided by eSign is restricted by a PIN. Only the holder of the electronic signature / the seal issuer to whom it is issued must know and use the PIN to access the smart card. After entering the wrong PIN three times, the smart card is blocked.

The electronic signature holder / seal issuer who has been issued with the QCQES must take the necessary action to prevent any other person from receiving the PIN information.

6.5. Using the private key

In every case of using the private key and the qualified certificate, the smart card is required to be inserted into the card reader. To prevent the unauthorized use of the private key and qualified certificate by others, the card should not be left unattended on the card reader. If the PC is not to be used for a longer period of time, the smart card should not be left in the reader and the PC should be shut down and / or adequate measures taken to prevent unauthorized access next to it with hardware and operating system resources.

6.6. Loss or destruction

If the private key is lost or destroyed, the electronic signature holder / print creator / person to whom it is issued loses the opportunity to use the Qualified Certificate. ESign is not able to recover the lost or

destroyed key pair because it does not have the ability to copy it. When it is generated on a smart card, the private key can not be exported by it in any way. Losing or destroying the smart card on which the private key is stored leads to the inability to use the electronic signature / electronic seal further.

6.7. Signing/seal issuing

When signing / seal issuing, the electronic signature holder / seal issuer uses his / her private key and qualified certificate to create the electronic signature / electronic seal. The electronic signature holder / seal issuer should take the necessary measures to prevent others from gaining access to the media containing the private key as this will compromise the private key.

6.8. Encryption and decryption

Encryption uses the public key of the subscriber, and when decrypting the private key corresponding to it. When performing the decryption operation of an encrypted electronic document, the subscriber uses the private key for this purpose. The subscriber and all stakeholders must be aware that when the private key that is decrypted is lost or destroyed, the electronic documents processed in that way become unavailable.

6.9. Cryptographic algorithms

The use of cryptographic algorithms that do not provide a sufficient level of security for the needs of subscribers is a breach of security requirements. At present, worldwide practice is considered safe and it is recommended to use RSA signing algorithm, SHA1 (160bit) for hash and 3DES algorithm for data encryption.

Subscribers should only use algorithms with a high level of security and in accordance with the regulatory framework governing their use.

6.10. Applied Software

The use of qualified certificates for electronic signature / electronic printing is done through software applications. Subscriber and Trustworthy parties should use only licensed software of proven origin that complies with generally accepted practice in information security standards. Using unauthorized software is a violation of security requirements.

7. Qualified certificate status

This section presents the rules for updating and verifying the status of qualified certificates issued by the SEP Bulgaria.

7.1. Issuance and validity of the qualified certificate.

SEP Bulgaria will issue a qualified certificate after satisfying the request for a qualified certificate. Qualified certificates are valid when issued by SEP Bulgaria and accepted by subscribers.

7.2. Acceptance of qualified certificate by the subscriber

The subscriber accepts that the qualified certificate has been implicitly accepted by him / her under either of the following conditions:

- the subscriber's approval is displayed on SEP Bulgaria online or via an e-mail sent by the subscriber;
- qualified certificate is used by the subscriber for the first time;
- upon expiration of 3 days from the date of issue of the qualified certificate, if the subscriber has not made a claim regarding the content of the qualified certificate within this period.

7.3. Trusted electronic signatures / electronic stamps

The final decision on whether to trust the electronic signature / electronic seal must be taken by the verifier in the following circumstances:

- The electronic signature / electronic seal was created at a time when the qualified certificate was valid, which can be verified by reference to the validity of the qualified certificate;
- the examiner adopts the terms and conditions under which the signature of the signatory / issuer has been issued;
- trust is reasonable for the circumstances.

7.4. Suspension and termination of qualified certificates

The temporary suspension of a qualified certificate aims to temporarily suspend its use. Termination of a qualified certificate permanently stops the operation of the certificate. SEP Bulgaria temporarily suspends or terminates a qualified certificate in case of:

- existence of reasonable facts and circumstances showing that there is loss, theft, alteration, unauthorized disclosure or other compromise of the private key;
- the owner / issuer, respectively the subscriber has violated his / her obligations under the CPS;
- the performance of any CPS obligation has been delayed or failed because of a natural disaster, computer failure or communication or any other reason beyond the control of the person and as a result the information of another person is threatened or compromised;
- there is a change in the information contained in the qualified certificate of the subscriber;
- at the request of bodies specified in a legislative act.

7.5. Request for suspension or termination

The subscriber or body referred to in a regulatory act may request the suspension or termination of the qualified certificate. The identity of the applicant and his representative authority will be confirmed, depending on the nature of the requested action.

7.6. Effect of suspension or termination

For the period of temporary suspension or termination of the qualified certificate, its validity shall immediately be deemed terminated. The validity of the certificate shall be resumed upon expiration of the suspension period, upon lapse of the ground for suspension or at the request of the subscriber in accordance with the regulations.

7.7. Notification when stopping and terminating a qualified certificate

SEP Bulgaria notifies the subscriber of termination or suspension of the qualified certificate and of the reasons for termination or suspension by the means of communication it deems appropriate.

7.8. Termination of qualified certificate

Termination of qualified certificate is done by the SEP Bulgaria upon submission of a termination request by the Registration Body. To make this request, the operator of the Registration Body is required to ascertain the identity of the applicant / authorized / authorized representative of the applicant as well as the representative authority of the authorized / authorized representative of the applicant.

7.8.1. Grounds for termination

The grounds for terminating a qualified certificate may be, but are not limited to, the following:

(1) There are reasonable grounds and circumstances that indicate that there is loss, theft, alteration, unauthorized disclosure or other compromise of the private key.
(2) Termination of the representative power of the natural person against the legal entity entered in the content of the certificate.
(3) Termination of the subscriber's legal entity.
(4) Death or imprisonment of the individual.
(5) Establish that the qualified certificate was issued on the basis of incorrect data.
(6) In the event of a change in the information originally filed and contained in the qualified certificate of the subscriber.
(7) In case of failure of the obligations of the subscriber under the certification service contract.
(8) At the request of the subscriber, after verification of the applicant's identity and representative authority.
(9) The operation of all qualified certificates issued by the SPS is terminated unconditionally upon termination of SEP Bulgaria’s activity.

7.9. Suspension of qualified SEP Bulgaria’s certificates

The performance of a qualified certificate issued by SEP Bulgaria may be suspended, provided the relevant grounds are available, for the time required by the circumstances but for no more than 48 hours.

For the period of temporary suspension of the qualified certificate, the same is considered invalid.

7.9.1. Grounds for Suspension

The performance of a qualified certificate issued by SEP Bulgaria may be suspended:

(1) Upon request of the subscriber. The request may be filed both with the Registration Body and other means of communication, including telephone, e-mail.

(2) At the request of a person who, in the circumstances, appears to be aware of security breaches of the private key, such as a representative, partner, employee, family member, etc.

(3) By order of the Supervisory Authority - in case of imminent danger for the interests of third parties or in the presence of sufficient data for violation of the law.

7.9.2. Resumption of Qualified Certificate

The validity of a qualified certificate is resumed upon expiration of the standstill period when the reason for the suspension or at the request of the subscriber is dropped after the SPE or the Supervisory Authority is satisfied that he has learned the reason for the suspension and that the request for resumption is made as a result of learning. The Certifying Authority resumes the validity of the qualified certificate by removing it from the list of suspended and discontinued certificates

7.10. Grounds for resuming the validity of a qualified certificate

(1) Upon the order of the Supervisory Authority - when the reason for the suspension of the act is an order of the Supervisory Authority.
(2) After the expiration of the validity of the certificate.
(3) At the request of the subscriber.

8. Terms and conditions for use of Qualified Certificates

This part of the document describes the legal guarantees, grounds, and limitations associated with qualified certificates issued by the SEP Bulgaria.

8.1. Administrative order and conditions for use of qualified certificates

SPE issues qualified certificates to individuals and legal entities. Individuals who request and use qualified certificates of the eSign QES Natural type are governed by the terms and conditions of use specified in this document and in the ESIGN CPS. The terms and conditions for the use of qualified

certificates issued to legal entities (eSign QESeal) or to individuals associated with legal entities (eSign QES Delegated), it is expedient for the legal entity - a subscriber to develop an internal normative document In the framework of the entity's internal rules, this document should govern the scope, rights, obligations and responsibilities of the legal entity's employees with regard to their electronic statements and the use of qualified certificates by them.

8.2. Identity

Persons using qualified certificates and relaying parties should be familiar with the rules and procedures for identifying subscribers of qualified certificates issued by SEP Bulgaria, which will allow them to make the relevant decisions on the use, verification and trust of electronic signatures / electronic seals and qualified certificates.

8.3. Requirements for Qualified Certified Applicants

Before or during the qualified certification process, qualified certified applicants do the following:

- apply for a qualified certificate and accept the terms of the trust services agreement and SPS;
- provide evidence of their identity / representative authority according to SEP Bulgaria standard procedures.

8.4. Empowerment

Request for a qualified certificate of the SEP Bulgaria can be made personally or through a proxy / representative, depending on the type of qualified certificate and the conditions for its issuance. The authorization shall be evidenced by a notarized power of attorney, a current status document (where applicable) and other documents defining the legal relationship between the authorizing officer and the proxy / representative and representative and his / her rights.

8.5. Key pair generation

SEP Bulgaria registration bodies have overall responsibility for the safe generation of the key pair of the subscriber when a secure signature / electronic signature (smart card) security mechanism is used for this purpose. Depending on the type of qualified certificate and the conditions for its issuance, the subscriber may be present in the generation process. When generating a key pair for qualified certificates for qualified electronic signature / qualified electronic seal, a secure signature / electronic seal creation device with the appropriate required security level in accordance with Regulation (EU) No 910/2014 should be used. In cases where the key pair is generated at the holder / issuer or subscriber, the registration body checks the security level requirements of the device to create an electronic signature / seal and verify compliance with the cryptographic requirements.

8.6. Key pair protection

Subscribers are solely responsible for preventing the compromise, loss, disclosure, modification, or other unauthorized use of their private key by properly protecting their personal identification code (PIN) for pairing and / or physical access to the media holding the key pair.

In cases where the subscriber is a legal entity, the responsibility for protection of the key pair is the responsibility of the holder of the electronic signature, respectively the originator.

8.7. Delegating responsibilities for the private key

Subscribers are fully responsible for actions or omissions by authorized persons or their partners that they use to store, store, or destroy their private keys.

8.8. Obligation regarding the information provided

In all cases, and for all types of qualified certificates issued by SEP Bulgaria, the subscriber (and not SEP Bulgaria) bears a permanent obligation to monitor the accuracy, correctness and completeness of the information provided when the qualified certificate is issued and immediately notify SEP Bulgaria about any changes.

8.9. Publishing information

Public information related to SEP Bulgaria's activities may be updated periodically. Such updates will be noted by appropriate version numbering and date of publication for each new release.

8.10. Standards

SEP Bulgaria assumes that the subscriber's software is compliant with the X.509v3 standard and other applicable standards and meets the requirements set by CPS. SEP Bulgaria cannot guarantee that the subscriber software will support and perform the controls required by SEP Bulgaria. If necessary, the subscriber may seek appropriate advice.

8.11. Selection of cryptographic methods

The Parties accept that they are solely responsible and have made an independent decision on the choice of encryption / electronic signature / electronic software, hardware and algorithms including their respective parameters, procedures and techniques in accordance with the requirements of Regulation (EC) No 910 / 2014.

9. eSign's list of suspended and terminated certificates

ESign provides public access to suspended and terminated qualified certificates in order to increase the level of trust in its services. Consumers and relying parties are advised that they must always check the suspended qualified certificates before deciding whether to trust the information entered in a qualified

certificate. SEP Bulgaria updates its lists of suspended and terminated qualified certificates automatically at each event or every three hours.

SEP Bulgaria publishes and provides access to documents related to certification services, including CPS, as well as any other information it considers important for the services it provides.

9.1. Profile of the list of suspended and terminated certificates

field	Value, subfield	
version	Version 2	
issuer (Distinguished Name)	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP
	CN	{eSign Sep Root CA, eSign Sep QES CA}
	Street	1 Zlatovrah Str.
	E	eSign@sep.bg
thisUpdate	Issue Date of the list of terminated certificates	
nextUpdate	Issue Date of next list of discontinued certificates	
signature	Electronic signature of the issuer of the list of terminated certificates	
CRLNumber	Number of a monotonously rising line	
AuthorityKeyIdentifier		
revokedCertificates	userCertificate	Serial number
	revocationDate	Date of placement in the list of terminated certificates

	crlEntryExtensions	{unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn}

9.2. Indication of the reason for termination / suspension of a certificate

(1) keyCompromise - owner / creator private key compromised
(2) ACompromise - a compromised private key of the Operator Certification Authority of the Provider
(3) affiliationChange - changed Holder status towards another person - change in representative power, withdrawal of representative power, termination of employment relationship, etc .
(4) superseded - the certificate is replaced by another
(5) certificateHold - the certificate is temporarily suspended

10. Obligations of the subscriber

Unless otherwise stated in the CPS, SEP Bulgaria's subscribers are fully responsible for the following:

- have knowledge of the use of qualified certificates;
- provide true, accurate and complete information to SEP Bulgaria;
- to familiarize themselves and accept the terms and conditions of CPS of SEP Bulgaria and related documents published in SEP Bulgaria's repository;
- use qualified certificates issued by SEP Bulgaria only for legitimate purposes and in accordance with the CPC of SEP Bulgaria;
- notify SEP Bulgaria or the SER registration body about changes and incompleteness in the information provided;
- discontinue the use of the qualified certificate if any part of the information proves to be outdated, altered, inaccurate or incorrect;
- suspend the use of the qualified certificate if it has expired and uninstall it from the applications or devices in which it was installed;
- prevent the compromise, loss, disclosure, modification or other unauthorized use of the private key that corresponds to the public key published in the qualified certificate by reliably protecting the personal identification key (PIN) for working with the key pair and / or physical access to the media , holding the key pair;
- request termination of the qualified certificate if there are doubts about the integrity of the certificate issued;

- request termination of the qualified certificate if some of the information included in the certificate proves to be outdated, altered, inaccurate or incorrect;
- for actions and omissions of third parties to whom they have unlawfully provided their private key;
- refrain from submitting to SEP Bulgaria materials of defamatory, obscene, pornographic, offensive, fanatical or racist nature.

11. Accuracy, correctness and completeness of the information

The subscriber bears full responsibility for the accuracy, completeness and completeness of the information he provides for use in issuing a qualified certificate according to the CPS.

12. Liability of the subscriber to the relying party

Without limiting the other obligations of the subscriber specified in the CPS, subscribers are responsible for any false statements made by them when issuing the qualified certificate to third parties who reasonably trust the information specified there.

13. Trust at your own risk

The responsibility for the evaluation and confidentiality of the SER's information and website lies with the parties using this information.

The parties agree that they have received the necessary information to decide whether to trust the information specified in the qualified certificate.

14. Obligations of SEP Bulgaria

To the level specified in the relevant section of the CPS, SEP Bulgaria undertakes to:

- comply with the CPS and its internal or public policies and procedures;
- comply with Regulation (EU) No 910/2014 and national law;
- provide infrastructure and certification services;
- provide for reliable mechanisms, including the key generation mechanism, the secure signature-creation mechanism and procedures for sharing secret parts with respect to its own infrastructure;
- notify the parties in case of compromise of their private keys;
- publicly provide the procedures for declaring the different types of qualified certificates;
- issue and renew qualified certificates in accordance with the CPS and fulfils the obligations set out therein;
- Issue and renew qualified certificates upon receipt of a request from the registration body in accordance with the CPS;

- upon receipt of a request for termination of a qualified certificate by the registration body terminates the certificate in accordance with the CPS;
- provide support for subscribers and relying parties as described in the CPS;
- terminate, suspend and resume qualified certificates in accordance with the CPS;
- provide information on the expiry and renewal of the qualified certificate in accordance with the CPS;
- provide public access to the CPS and its current documents.

15. Other warranties

In addition, as set out in Regulation (EU) No 910/2014 and national law, SEP Bulgaria does not provide guarantees for:

- the accuracy, authenticity, completeness or correspondence of any unverified information contained in the qualified certificate or distributed by or on behalf of SEP Bulgaria as specified in the relevant product description in the ESign's CPS;
- the accuracy, authenticity, completeness or consistency of any information contained in test or demonstration qualified certificates issued by the CPS;
- presentation of information in the qualified certificate, unless otherwise specified in the relevant product description in the CPS;
- although SEP Bulgaria has obligations to terminate a qualified certificate, it is not responsible if it cannot terminate it for reasons beyond its control;
- validity, accuracy and availability of list with suspended or terminated qualified certificates, supported by third parties unless this is explicitly indicated by SEP Bulgaria.

16. Intellectual property rights

ESign holds the intellectual property right concerning the database, web sites, qualified certificates of SEP Bulgaria and any other publications that have been made by SEP Bulgaria including CPS.