“SYSTEM FOR ELECTRONIC PAYMENTS BULGARIA/SEP BULGARIA” JSC

eSign User Guide

Version 2.1

21.06.2013

CHAPTER I

GENERAL CONDITIONS

"System for Electronic Payments Bulgaria/SEP Bulgaria" JSC (as stated below as SEP Bulgaria) is an accredited provider of certification services (CSP) according to §41 of Act for amendments and alternations to the Electronic document and electronic signature Act, promulgated in " State Gazette" N. 100 from 2010r.

This User Guide (Guide) unifies " The practice for providing certification services" of SEP Bulgaria (here and further mentioned as Practice) and „The policy for providing certification services " of SEP Bulgaria (here and further mentioned as Policy), and gives details of the regulations concerning the certification practice of SEP Bulgaria and also describe the processes for providing certification services and the area of implementation of the certificate for electronic signature a s a result of these services.

I. Character of the document

The Guide accompanied by the Contract concluded by the Client are giving the shape of the contractual relations between SEP Bulgaria and the Client, in the terms of which the last one has the right to use the certification services provided by SEP Bulgaria. The Guide has got General Terms character and has abidance regime for SEP Bulgaria and concerning the Client –after the signature of the exact contract for providing of certification services.

The Guide is a public document for CSP and is supposed to be introduced to the Communications Regulation Commission and to all interested parties .The Guide as well as the documents of public character are available in electronic form at the electronic page of SEP Bulgaria.

II. Content and details of the document

In its capacity as CSP- SEP Bulgaria - acting at territory of Republic of Bulgaria has developed the current Guide which includes:

- „Practice for providing certification services";
- „Policy for providing electronic services";

The Guide is developed according to EDESA, under law acts to its execution and the universally accepted international standard RFC 3647 Internet X.509 Public Key Infrastructure: Certification Policy and Certification Practices Framework.

The document „Practice for providing certification services" describes in details:

- The range and the applicability of the offered by SEP Bulgaria certification services including time stamps;
- The technology for issuing and management of Certificates for QES;
- The form, the terms of action and validity of the issued Certificates for QES;
- The required documents for acceptance and check of requests for providing certification services;
- The documents and the data preserved by CSP in providing certification services;
- The sustained algorithms for electronic signature and data protection;
- The obligations and responsibilities of all parties taking actions in activities of issuing and management of Certificates for QES;
- The regulations and procedures executed by CSP at issuing certificates for QES;

- The regulations and procedures executed by CSP in case of suspension, reactivation or revocation of Certificates for QES.

The document „Policy for providing certification services" describes the policy of issuing of certificates by CSP and the types of certification services provided by SEP Bulgaria including the services for issuing certificates for time stamp.

The Policy of SEP Bulgaria describes the general rules during the execution of the activities of SEP Bulgaria concerning providing of certification services through the definition of the details and the character of the activity, the participants in the certification process, their obligations and responsibilities, the procedures for checkup of the customer's information, the field of application of QES.

The Policy defines the level of trust to issued by SEP Bulgaria Certificates for QES. The Practice of SEP Bulgaria shows the way to be reached and guaranteed those levels of trust.

III. Terms of action and suspension of the act of the document

1. Terms of action

The rules of the Guide as well as the included in it „Practice for providing certification services" and „Policy for providing certification services „ are valid until their change or until publication of information for invalidity by SEP Bulgaria.

2. Suspension of the action of the Guide

The action of the Guide is suspended by suspension of the activity of SEP Bulgaria as CSP.

3. Legal consequences resulting from the suspension of the action of the document

After the suspension of the act of the Guide there are enforceable orders for the obligations of SEP Bulgaria for maintenance of the archives of the documents and certificates in the scope and the period described in the Practice.

IV. Notice and communication

Announcements to SEP Bulgaria related to the activities for providing certification services are supposed to be sent in written form at address:

„System for electronic payments Bulgaria/SEP Bulgaria" JSC

1 „Zlatovrah" str.1

1164, Sofia

Or by e-mail: eSign@sep.bg.

Notifications to the customers of SEP Bulgaria are sent to the provided by them in the Contract e-mail address.

In cases, when there is necessity to send written announcement or documents, SEP Bulgaria send it by e-mail depending on the character of the announcement or document as a letter with receipt or by delivery service.

V. Amendments

SEP Bulgaria in case of need makes amendments to the Guide and informs Communications Regulations Commission for every happened change.

Each change in the Guide comes into force in the terms of 7 (seven) days by its publication on the electronic page of SEP Bulgaria. The changes in the Guide have binding action to all Client s and users who at moment of coming into force of the changes use provided by SEP Bulgaria certification services and don`t declare their rejection by the set of rules provided below.

Each Client has the right to request suspension of the provided by SEP Bulgaria certification services by explicitly written notification in the terms of 7 (seven) days from the moment of coming into action of the changes in the Guide. The last one is not applicable when the changes comes from the applicable legislation, from the act of other authority or provide more beneficial clauses for the Client s.

VI. Settling a dispute

In case of dispute related to the provision of certification services by SEP Bulgaria, the parties concerned file a claim to the Executive director of SEP Bulgaria at the following address:

„System for electronic payments Bulgaria/SEP Bulgaria" JSC

1 „Zlatovrah" str.1

1164, Sofia

The users of SEP Bulgaria can send claims at address: esign@sep.bg. For the purpose the user has to sign his complaint with valid QES. Complaints are considered to be received only if they are signed properly.

Within 30 (thirty) days of its receipt, the complaint will be reviewed and a written reply of the Executive Director is sent to the Client.

VII. Applicable legislation

For legal matters which don`t stand in the scope of the current Guide but are related to the provision of certification services is applicable the corresponding European legislation and the operative Bulgarian legislation.

VIII. Final provisions

1. Succession

The rights and obligations of SEP Bulgaria pointed out in this Guide can be transferred by mutual agreement of the parties, by the force of law, as a result of transform or by other method in case that such transfer is performed according to the terms of the Guide.

2. Interpretation

In case of delivery of certification services the Guide should be interpreted according to the legislation in force, the generally accepted business practices at the certain circumstances and the use of the services by function.

In case that some of the clauses of the current Guide are invalid that doesn`t mean that other clauses or parts of the Practice or Policy are invalid or it will not make the Contract for providing certification services with the Client,

invalid.The invalid clause will be replaced by certain legal regulation of EDESA and the subordinate legal regulations by its enforcement.

3. Force major

The users of certification services and SEP-Bulgaria as well don`t take responsibility for non-feasance as a result of the current Guide (unless there is other provision in the legislation) due to force major. The party who is a victim of force major is obliged to inform immediately the other party and also to take a good care to lessen the consequences of the non-feasance.

4. Jurisdiction

All arguments, which has arisen on the occasion of the providing of certification services of SEP Bulgaria which cannot be solved by negotiations between the parties will be raised to the competent court in Sofia town.

5. Regulations

The relations between SEP Bulgaria and the Clients of CSP are regulated by the current Guide according to:

[1] EDESA: „Electronic document and electronic signature act";

[2] OORCSP: „Ordinance on the order of registration of the providers of certification services";

[3] OACSPOSRCSP: „Ordinance on the activities of the providers of certification services, the order of its suspension and for the requirements at providing certification services";

[4] ORACCQES: „Ordinance on the requirements to the algorhytms for creation and validation of a qualified electronic signature";

[5] OOCPARCSP: „Ordinance №1 from 10.03.2011 on the order and the conditions, preservation and access to register of providers of certification services";

[] „Directive 1999/93/EC of the European Parliament and OF the Council, of 13 December 1999, on a Community framework for electronic signatures";

[7] Decision: „Commission Decision of 14 July 2003, On the Publication of Reference Numbers of Generally Recognised Standards for Electronic Signature Products in Accordance with Directive 1999/93/EC of the European Parliament and of the Council"

[8] RFC 3280: „Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile";

[9] RFC 3628: "Requirements for Time-Stamping Authorities";

[10] RFC 3647: „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework";

[11] RFC 3739: „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile";

[12] ETSI TS 101 456 V1.4.3: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates" technical specification (2007-05);

[13] ETSI TS 101 862 V1.3.3: "Qualified Certificate profile" technical specification (2006-01);

[14] ETSI TS 102 023 v.1.2.1: "Policy Requirements for time-stamping authorities"(2003-01);

[15] ANSI X9.79: "Public Key Infrastructure (PKI) - Practices and Policy Framework";

[16] CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1 System Security Requirements".

IX. Definitions and abbreviations

1. Definitions

The used in this Guide terms will have the following meaning:

Author/Author of electronic statement	The natural person who is considered to be the author of the electronic statement.
Author/Holder of electronic signature/qualified electronic signature	The author/The holder registered in the certificate of electronic signature/qualified electronic signature.
Data for validation of the signature	Data like codes and public cryptographic keys used for validation of the electronic signature.
Real signature	Electronic signature which can be verified through valid Certificate for QES.
Relying party	Receivers of documents signed with qualified electronic signature who take action trusting into the Certificate for relevant qualified electronic signature and/or into the electronic signatures checked by the public key from this certificate.
Contract	Contract for certification services between SEP Bulgaria and a Client.
The electronic page of SEP Bulgaria	Electronic page http://eSign.bg/
Electronic statement	Statement in verbal or non-verbal form introduced in digit form through generally accepted standard for transformation, deciphering and visual presentation of the information.
Applicant	Natural person who requests a certification service.
Identificator of an object (OID)	Unique sequence of whole numbers which applies to the registered object.
Qualified Electronic Signature (QES)	Qualified electronic signature is an enhanced electronic signature which: • Is accompanied by certificate for qualified electronic signature issued by CSP responding to the regulations of art. 24 from EDESA and certifying between the author and the public key for check of the signature and • Is created by device for secure creation of the signature.

Client	Natural or juridical person who has contract with SEP Bulgaria for providing certification services.
Mechanism for the check of signature	Configured software or hardware used for the application of the data for check of the signature.
Guide	User Guide
Online	Regime under which the person is related to network or to the server of an Internet provider.
Personal Identification Number (PIN)	Sequence of symbols which serves as identificator of the holder of the means for identification.
User	Client and/or applicant and/or relying party.
Attorney	A person empowered by the Holder /Author to ask for certification services or to take action related to the Contract for certification services or change of status of the issued Certificates for QES.
Holder /Holder of electronic statement	The natural/juridical person on behalf of who is posted the electronic statement.
Certificate for qualified electronic signature (QES Certificate)	The certificate is an electronic document issued and signed by the provider of the certification services which may have the following containment: • Indication that the certificate is issued for qualified electronic signature; • The name and the address of CSP and also directions for the state in which he has established his activity; • The name or the pseudonym/alias of the Author of the electronic signature; • Special attributes related to the Author if the certificate is issued for certain purpose and also if the provider has policy for issuing a certificate with entry of such attributes; • The public key relevant to the private held by the author for the creation of the qualified electronic signature; • The enhanced electronic signature of SEP Bulgaria in its capacity as CSP; • The terms of action of the certificate; • The limits of the action of the signature regarding the purposes and/or the value of the transactions if the certificate is issued with limits to the certification action; • The unique identifiable code of the certificate; • Indication for accreditation of the provider.
Certification process	The acts of issuing and management of certificate for qualified electronic signature, the services for validation of certificates for qualified electronic signatures as well as the acts of the relying parties in relation with the certificates for qualified electronic signatures.
Certification services	The services for issuing, modification, suspension, reactivation,

	revocation/termination and maintenance of certificate for qualified electronic signature as well as the services for validation of certificate qualified electronic signature and the time stamp services.
Secure signature creation device (SSCD)	Mechanism for creation of electronic signature which corresponds to the requirements of art. 17, par. 1 of EDESA.
Enhanced electronic signature	Enhanced electronic signature is an electronic signature which: • gives possibility for identification of the author; • is related to the author by unique way; • is created by means which are under the control only of the author and • is related to the electronic statement in a way which ensures the establishment of all further changes.
Online Certificate Status Protocol (OCSP)	Internet protocol for online check of the status of issued certificate for electronic signature.

2. Abbreviations

The used in this Guide abbreviations will have the following meaning:

CSP	Certification services provider
ES	Electronic signature
QES	Qualified electronic signature
Policy	Policy for providing certification services
Practice	Practice for providing certification services
RA	Registration authority
CS	Certification services
CES	Certificate for electronic signature
CA	Certification authority
EES	Enhanced electronic signature
CS	Certification services
OID	Object Identifier
OCSP	Online Certificate Status Protocol
SEP ROOT CA	Root certificate for certification of SEP Bulgaria
eSign QES CA	Operational certificate for certification of SEP Bulgaria

SSCD	Secure Signature Creation Device
TSA	Time Stamp Authority

CHAPTER II

PRACTICE FOR PROVIDING CERTIFICATION SERVICES

I. Overview

„Practice for providing certification services“ is a major part of the documents for the activities of the Certification authorities, Registration authorities, the Clients and the Relying parties.

The Certification services of SEP Bulgaria are provided by hierarchy of Certification authorities signing the issued types of certificates for QES, Time stamps and the result of the online validation for the status of Certificates for QES.

SEP Bulgaria has got one Operational Certification authority hierarchal situated under the Root Certification authority. The Operational certification authority signs the different types of Certificates for QES issued by CSP – SEP Bulgaria and the certificate for the online validation.The Root Certification authority signs the Operational Certification authority and the certificate for Time stamp.

Certificates for QES issued by SEP Bulgaria include in their content an identifier of the policy according to which they have been issued.

II. Parties in the certification process

„The practice for providing certification services“ is a mutual regulative document concerning all the participants in the process of providing certification services from SEP Bulgaria and describes the process of providing certification services, the interaction between RA , CA, Clients and Relying parties. The practice is a leading document when there are checks of the activity of CSP and is responding to the activities of the Certification authorities – SEP Root CA, eSign QES CA and the Registration authorities – on one hand and on the other hand – to the relations with the Authors/Holder, entered in Certificates for QES and with Relying parties.

SEP Bulgaria provides certification services to all juridical and natural persons accepting the rules and practices described in this document. The application of these rules and practices has the purpose to ensure the declared level of security while providing certification services.

1. Certification authorities

SEP Bulgaria is providing certification services through hierarchy of Certification authorities and network of Registration authorities by issuing and managing Certificates for QES.

SEP Bulgaria in its capacity as CSP publishes information for the status of the Certificates for QES and gives it to the Relying parties for the purposes of QES validation.

1.1. Root Certification authority

SEP Root CA issues basic enhanced electronic signature (EnES) of itself and operational enhanced electronic signatures to other CAs belonging to the CA's hierarchy of SEP Bulgaria. SEP Root CA is functioning on the basis of EnES issued by himself. In this EnES is not included OID for the policy towards which are issued and managed EnES. The lack of identifier of the policy should be interpreted as a lack of limitations regarding the policy towards which CA – SEP Root CA issues certificates.

SEP Root CA is an originating point of trust for all users of certification services of SEP Bulgaria. That means that the procedure of certification for each issued QES in the hierarchy of CSP begins from EnES of CA – SEP Root CA.

The Root CA of SEP Bulgaria – SEP Root CA issues EnES for:

- himself – SEP Root CA;
- The Operational CA – eSign QES CA;
- SEP TSA – the certificate for validation of objects with certified time (TimeStamp).

1.2. Operational Certification authority

Operational CA of SEP Bulgaria is eSign QES CA. The operational CA issues certificates for QES according to the „Policy for providing of certification services" of SEP Bulgaria to natural or juridical persons. The Operational CA includes in the issued certificates for QES identifiers for objects in order to identify the issued certificates from different type according to this policy.

The identifiers for the objects are:

SEP Bulgaria JSC	SEP Root CA	eSign QES CA	Objects/Certificate types	
1.3.6.1.4.1.30299	2	5	1	eSign Qualified Private
			2	eSign Qualified Organization
			3	eSignQualified Profession
			4	eSign TSA
			5	eSign OCSP

The certificates for QES issued by the operational CA contain identifier of the policy towards which they have been issued.

The operational CA issues Certificate for check of online response for the status of issued certificate for electronic signature (OCSP).

SEP TimeStamp certificates are issued to juridical and natural persons – users of CSP. The certificate for time has official certificatory power after being enrolled in the managed by SEP Bulgaria register available at address http://tsa.sep.bg

The certificate includes identifier of policy pointed out in the scale:

Oobject	Identifier of policy
SEP TSA	1.3.6.1.4.1.30299.2.1.5

The Operational Certification authority eSign QES CA issues certificate for electronic signature which is used for online validation of the status of QES Certificate.The certificate includes identifier of policy pointed out in the scale:

Oobject	Identifier of policy
eSign OCSP	1.3.6.1.4.1.30299.2.5.5

2. Registration authorities

The Registration authorities are part of the infrastructure of SEP Bulgaria in its capacity as CSP. RA represent SEP Bulgaria while contacting with Clients and they are functioning according to the rights authorized to them by CA as regards to the check of identity respectively the authentity of the Author/Holder and registration of requests for issuing or management of the Certificates for QES.

CSP issues Certificates for QES after an identification of the applicants for the certification services. In this relation SEP Bulgaria provides its services through a network of RA who has the following functions:

- Accept, check, prove or deny the Requests for issuing of Certificates for QES;
- Accept, check, approve or deny the Requests for management of Certificates for QES;
- Take part in all stages at the identification of the Applicants, Authors and Holder of certification services and check of identity;
- Making contracts for certification services provided by the CSP - issuing, maintenance and management of certificates for QES with Holder on behalf of SEP Bulgaria;
- Have other activities related to the provisioning of certification services described in the policies, practices and procedures of CSP.

The Registration authorities act on behalf of SEP Bulgaria according to its policies, practices and procedures.

RA accepts checks and approves or denies Requests for issuing, management and maintenance of Certificates for QES.

At the check of identity respectively of the Holder /Author the operators of RA identify directly or indirectly persons that will be issued certificates for QES by using methods of identification giving the same level of security just like the physical identification.

SEP Bulgaria is making a contract with RA (in the cases when the particular RA is an unit outside of the legally-organizational structure of SEP Bulgaria), by the power of which the activities proceed,as stated above, and Guide of CSP is a part of this contract.

Each person may function as RA of CSP – SEP Bulgaria, after he declares this and implements the conditions, resulting from the regulations of CSP.

The list of RA, who is authorized by SEP Bulgaria is public and it is available at the electronic page of SEP Bulgaria.

3. User

The users of Certification services of SEP Bulgaria are Clients and Relying parties.

3.1. Author

Author of the electronic statement –the natural person who is pointed out as his author in the statement.

3.2. Holder

Holder of the electronic statement –the person on behalf of whom is performed the electronic statement.

3.3. Distinction of Holder and Author

In case of issuing a Certificate for QES for natural person, the Author and the Holder registered in the Certificate ccoincide.

By issuing a Certificate for QES for juridical person, in the Certificate as Holder the juridical person is registered and as Author – the respective person who has come into power to use the issued Certificate.

3.4. Relying parties

The parties are recipients of documents signed with QES who are taking actions trusting to the Certificate for the particular QES. The relying party is responsible for the check of validity of the certificate for QES.The decision for the acceptance of the authenticy of the electronic statement signed with QES is taken by the relying party each time at receiving of such.

The Relying parties estimate if the type of the Certificate for QES and the warranties related to it are enough for purposes which it is used for. The responsibility of the Holder is to know the requirements of the Relying party and the use of responding to the respective requirements type of certificate for QES.

III. Providing of Certification services by SEP Bulgaria – range and applicability

SEP Bulgaria issues certificates for qualified electronic signature, certificates for time and certificates for electronic signature used for check of objects.

1. Certificates for qualified electronic signature

Certificates for qualified electronic signature can be used for specifying the authorship of electronic statements so they give significance of the electronic signature of an autographic signature respecting to all including state authorities or authorities of local administration.

The certificates for qualified electronic signatures, issued by SEP Bulgaria are the following types: eSign Qualified Private, eSign Qualified Organization и eSign Qualified Profession.

2. eSign Qualified Private certificate (eSign for natural persons)

Certificate of the type SEP Qualified Private is issued only to natural persons and is used for confirmation of the agreement/identity of the natural person during participation in electronic exchange like web based applications, signature of electronic documents and/or contracts, bank transactions and making statements in the sense of EDESA. On these types of certificates for QES, the Author and the Holder is the same person.

3. eSign Qualified Organization certificate (eSign for juridical persons)

Certificate of the type eSign Qualified Organization is issued to juridical persons and is used for confirmation of the agreement/identity, respectively the identity of the juridical person when participating in electronic exchange like web based applications, signature of electronic documents or/and contracts,bank transactions and making statements in the sense of EDESA. The Holder and the Author are different from each other when the author is a natural person (empowered by law or by respective and explicit power of attorney by the juridical person to make statements on behalf of the Holder) and the Holder – juridical person.

The Author makes the statements on behalf and at the expense of the Holder.

4. eSign Qualified Profession certificate (eSign for free professions)

Certificate of the type eSign Qualified Profession is issued to natural persons and is used for confirmation of agreement/identity and professional pertinent making services by personal labor or practicing free profession during participation in electronic exchange like web based applications, signature of electronic documents and/or contracts, bank transactions and making statements in the sense of EDESA. The Holder and the Author of the statements coincide.

5. SEP TSA certificate (Certification of time)

Certificate of the type SEP TSA is used for confirmation the time of introduction of electronic signature created for definite electronic document.

The certificate for time is an electronic document signed by CSP which contains:

- The identifier of policy for issuing certificates for time containing in this Guide;
- The electronic signature introduced to the deliverer of the signed electronic document;
- The identifiers of the algorithms used for the creation of the electronic signature;
- The time of introduction of the electronic signature;
- The unique identification number from the certification of time
- The certificate for the qualified electronic signature of CSP.

IV. Used applications

Certificates for QES issued according to the Guide can be used with applications which respond at least to the following requirements:

- The applications are a suitable manner to manage the private and public keys and their use as well.
- The Certificate for QES and the associated public keys are used according to the definite function approved by SEP Bulgaria;
- They have built in mechanism for check of the status of the Certificate for QES, the certification chain and control of validity (for example of signatures, time and so on.);
- Use algorithms defined in „Ordinance for requirements to algorithms for creation and of qualified electronic signature";
- Introduce suitable information for the Certificates for QES and the application itself of the Author.

Information on the applications with which can be used Certificates for QES issued by SEP Bulgaria is published on the electronic page of SEP Bulgaria.

SEP Bulgaria doesn`t take responsibility for the usage of the issued Certificates for QES with applications not responding to the requirements as stated above.

V. Public register and information

SEP Bulgaria in its capacity as CSP runs a public electronic register (Register) in which SEP Bulgaria publishes certificates of CA from its hierarchy, the issued certificates for QES and information needful to the parties using certification services.

1. Published information

SEP Bulgaria publishes the following information:

- List of certificates for electronic signature from its hierarchy;
- List of the issued Certificates for QES;
- List of the issued Certificates for time;
- List of the revoked Certificates for QES (CRL);
- Previous and actual versions of the documents regulating the activity of CSP;
- User Guide;
- Instructions describing the way of the usage of the electronic signature;
- Price lists for the services provided by CSP;
- Other information which can be changed and modified in real time.

2. Regularity of publishing the information

SEP Bulgaria maintains the information stated above by making it actual through the following regularity:

- User Guide – according to described in Chapter I, part V, the requirements of EDESA and the subordinate acts;
- The lists of the issued and revoked certificates of the Root CA – at every event happened or automatically, at least once a year when in the frames of this period there hasn`t been an event of issuing, suspension, reactivation or revocation;
- The list of the issued and revoked Certificates for QES of the Operational CA – at each happened event or automatically, on every three hours when in the frames of this period there hasn`t been an event of issuing, suspension, reactivation or revocation;
- Other information – in case of change.

3. Access to public register

SEP Bulgaria runs public electronic register (Register) of the issued by it Certificates with X.500 and LDAP based access.

The access to the Register and the containing in it information is public.

The Author entered in the Certificate for QES has the right to restrict the public access to the information in the issued Certificate by choosing so when filing a Request for Certification services. When the access is limited, SEP Bulgaria gives only the following information from the content of the Certificate:

- Serial number of the Certificate;
- Validity period of the Certificate;
- Status of the Certificate.

The access to information for the Certificates from the list of revoked certificates is not restricted by any means.

4. Preservation of the public register

SEP Bulgaria preserves its register by the way which ensures the following:

- The insertion of data to be made only by staff with particular authority;
- The initiation of change of data should be impossible;
- The possibility for authorized interference to be set to a minimum.

VI. Used names

1. Types of names

The Certificates for QES issued by SEP Bulgaria respond to the standard X.509 v3 and the following versions. CSP checks and approves the names of the Holder /Author according to standard X.509 v3. The basic name of the Holder /Author included in the Certificate responds to the lecture for Distinguished Name, according to recommendations X.500 *и* X.520.

In order to ensure easy communication by electronic way with Holder /Author SEP Bulgaria includes in the content of the Certificate for QES electronic address according to RFC822.

The names of the directories where the certificates for electronic signature are being preserved, "The list of the revoked certificates" and „The policy for providing certification services", as well as the names of CRL's distribution points are according to RFC1738 and scheme for names according to protocol LDAP – RFC 1778.

The issued by SEP Bulgaria Certificates for QES contain information as defined in art. 24 from EDESA.

The list with data which are included in the Certificates for QES and their interpretation is according to X.509 v3 and is introduced in chapter „Profiles of Certificates", List of the revoked certificates" and "OCPS".

2. Meaning of names

The Certificates for QES issued by SEP Bulgaria contain unique names with understandable semantics allowing the definition of the Provider (Issuer Distinguished Name) and identity of the Client (Subject Distinguished Name).

The certificates of the bodies of certification of the Provider contain unique names identifying the Provider – subject of the certificate.

The names included in the Client `s Distinguished Name contain the identification information for the Author/Holder.

The contents of the Distinguished Name is approved/assumed and checked by RA depending on Author/Holder and the type certificate and is approved by CA.

Distinguished Name contains a set of fields which description and abbreviations of the names is according to the recommendations RFC 3280 *и* X.520.

Distinguished Name of Holder/Author is confirmed by the operator of RA .

The specification with details and description of information and the respective fields for the different type of certificates are contained as stated below in the current Guide.

3. Rules for interpretation of the different name forms

The interpretation of the names of the fields in the Certificates for QES issued by SEP Bulgaria, is according to the different types of the Certificates (Profiles of the Certificates).

During the creation and the interpretation of the different Distinguished Names are being applied the general rules as stated below in Section VI of the current Guide.

4. Uniquity of names

In order to ensure uniquity of the issued Certificates for QES, SEP Bulgaria assumes a unique sixteen digit serial number for each issued certificate. The serial number is combination with Issuer Distinguished Name which precisely and uniquely identifies it. SEP Bulgaria guarantees also uniqity of the names and for the public electronic register.

5. Trade marks

The Clients don`t have neither the right to declare an issue of certificates with usages of names which are object to copyrights or related rights of third persons, nor the right to violate somebody else`s property or non-property rights. The holder of such rights declares that rights by introducing of appropriate document to RA in the process of introducing a demand for issuing of the corresponding Certificate. SEP Bulgaria doesn`t take responsibility when used names in the issued Certificates for QES violate somebody`s else rights on a trade name, trade mark, domains, copyrights and so on. The Client is responsible to CSP for all damages related to violations of the requirements of this p.5.

VII. Rules and procedures for providing and usage of certification services

1. Identification and authentication

This section introduces the general rules for check of the identity of the Author and the Holder applied by CSP while providing certification services. The rules are distinguished one form another depending on the type of information which is included in the Certificates. CSP is obliged to ensure the precision and the liability of this information at the moment of issuing a Certificate for QES (initial identification/authentication) and at the moment of entering a Request for management of Certificate for QES (following identification/authentication).

1.1. Initial identification and authentication of the person

Initial check of the identity of the Holder and the Author is initiated to:

- Initial presentation of Request for certification services at RA ;
- Registration and application for certification services by the electronic page of SEP Bulgaria.

1.1.1. Initial identification and authentication of the person at RA

1.1.1.1. Check of the identity of juridical persons – Holder of QES

RA requires the introduction of suitable documents which unconditionally and without any doubt confirm the identity of the juridical person pointed out in the certain Request for issuing a certificate who will be entered as Holder in the Certificate and of the natural person who represents the juridical person entered like Author in the certificate. The documents on the preceding sentence include:

- Identification document of the Author (ooriginal and certified by the Author copy as the copy remains to RA);
- Document for court registration of the juridical person (original and certified by the Holder copy as the copy remains to RA) – in case that the document is applicable concerning the type of the juridical person;

- Document for registration by number of identification (UIC) (original and certified by the Holder copy as the copy remains to RA) –– in case that the document is applicable concerning the type of the juridical person;
- Certificate of actuality of the juridical person issued in terms to one month from the date of submitting an application for certification services (original and certified by the Holder copy as the copy remains to RA).
- Document by model of CSP for explicit empowerment to the Author with delegation power by the Holder in case that the grounds of delegation power doesn`t follow from the law (ooriginal which remains to RA);
- Power of attorney attested by notary of the applicant of certification services in case that the Holder empowers his representative different than the author to declare certification services.

RA can check the needful data for the identification of the Holder by himself by using public registers but this right doesn`t cancel the obligation of the persons for presenting of the above stated documents.

The check of the identity of the juridical person can be achieved through:

- Representative of the juridical person with power of attorney to visit personally the office of RA ;
- Operator of RA to visit the main office of the juridical person;
- Operator of RA uses indirect method of identification giving the same level of security just like as direct physical identification.

If the check of identity is successful operator of RA proceeds to work on the data of the juridical person and the appropriate activities related to providing of certification services.

1.1.1.2. Check of identity of natural persons – Holder of QES

RA requires the presentation of suitable and appropriate documents which in unconditional and indisputable way confirm the existence and identity of the natural person who is entered as an Author and respectively Holder in the Certificate and its belonging to certain category of persons practicing free profession if the required Certificate demands this. The documents on the preceding sentence include:

- Document for identity of the Author (original and legalized by the Author copy as the copy remains in possession of RA);
- Power of attorney explicitly attested by notary following a model of CSP of the applicant certification services in cast that the Author entitles his representative to apply for the certification services;
- Appropriate document proving in indisputable way the affiliations of the person pointed out as a Holder to the relevant professional/branch organization (when the demanded certification services are for the usage of the Certificate by the type of SEP Qualified Profession (ooriginal and notarized by the Author copy as the copy remains in possession of RA);

The check of identity of the natural person can be achieved through:

- The natural person (representative with the power of attorney from the person) personally visits RA ;
- Representative of RA visits the natural person indicated in the Application;
- Operator of RA uses indirect method giving the same level of security to identification the same like with direct physical identification.

If the check is successful the operator of RA proceeds to processing of the data of the natural person and the relevant activities of providing of certification services

1.1.2. Initial identification and authentication of the person at registration for application of certification services by electronic way

The registration includes providing of data for the applicant of certification services by electronic way which allow SEP Bulgaria to makes it individual. The data on the preceding sentence include:

- Three names and pseudonym, and/or
- Personal data for the applicant, and/or
- Valid electronic address which may be used subsequently for communication with applicant.

The granted information at initial registration is preserved by SEP Bulgaria and may be used at acceptance of demands for certification services by CSP.

When there is a validation of the gathered data the person may proceed to next steps for demands for certification services

1.2. Succeeding identification and authentication of the person

Succeeding check of identity of the Holder and the Author is achieved at:

- Application of succeeding Requests for certification services to RA ;
- Initiation of process of Request for certification services by electronic way after accomplished initial registration.

1.2.1. Succeeding identification and authentication before RA

Succeeding identification and authentication before RA is accomplished at demand for management of existing certification services.

For accomplishment of identification and authentication RA makes check of the initially authenticated data for the Client in the due form of p. 1.1.1. from this Section and the data pointed out in the new Request.

1.2.2. Succeeding identification and authentication at registration by electronic way

Succeeding identification and authentication of the person is accomplished by PKI of SEP Bulgaria upon request for certification services.Demand for certification services may be submitted by initially registered Applicant in the due form of p. 1.1.2 from this Section.

In case that the registered Applicant owns valid Certificate for QES issued by CSP,the last one fills in electronically the Request for the relevant services and submits it using the valid Certificate. Together with the application should send electronically and following the procedure from the electronic portal of CSP and the needful documents for determine the identity of the Author/Holder and the other executable documents as stated above in p.1.1. „Initial identification and authentication before RA ".

In case that the registered applicant doesn`t own valid Certificate for QES issued by CSP, the submission of the Request and the attendant documents in this case is accomplished to RA due to the form provided in p. 1.1.1.

2. Unconfirmed in official way information

SEP Bulgaria makes check due to the form of section VII of this Chapter regarding to presented by the Applicant data according to the requirements of art. 5, par.1, p.1, б) of OACSPOSRCSP.

CSP may include in the content of Certificates for QES and data which cannot be confirmed in official way. Such data may be without being restrained only to:

- Electronic address for correspondence;
- Specific for the Author/Holder identifiers.

The officially unconfirmed information is included in the contents of the Certificate on basis declaration by the side the Author/Holder who submitted the Request.

SEP Bulgaria doesn`t take responsibility for the included unconfirmed information in the contents of the Certificate including impossibility by the Holder /Author to use the issued Certificate.

3. Confirmation of delegation

When providing certification services CSP checks the delegation power of the persons-being delegated or empowered by the Holder respectively the Author before taking actions of accomplishment of the declared services.

The delegation is checked on the basis granted by the Holder /Author official documents making visible the fact and the capacity of the delegation power.

CSP can collect the needful data for the confirmation of delegation when the same is based on legal provisions from publically available registers.

CSP doesn`t takes responsibility/doesn`t checks the right to the Holder for using of personal data of the Author. The responsibility for unlawful usage of personal data of the Author is taken by the Holder. The Holder is obliged to declare his right to use, protect and grant the personal data of the Author.

4. Conrtol on the pair of keys

If a person controls the private key when declares issuing of certificate for QES, CA and/or RA must be convinced that the granted for certification public key responds to the held by the person private key.

The check for the holding of the private key is accomplished through procedure for proving of possession of the private key.The procedure confirms that the public key of the Author responds to the private key and it's under its exclusive control.

At declaration of issuing a Certificate for QES, the Client `s cryptomodul SSCD generates a pair of keys and together with the developed by SEP Bulgaria PKI software forms electronic application in format PKCS #10 through which at creation of the Certificate is guaranteed the correspondence between the public key and the held by the Author private key.The electronic application is processed by CA and CA issues the required Certificate for QES.

At the time of generating the pair of keys the Client `s cryptomodul is controlled.

At declaration for issuing of Certificate for QES at RA the Client `s cryptomodul is passed to the Author. In this case CSP guarantees that the cryptomodul and the keys are granted to the Author in secure way.

At receiving of certification services in an electronic way the Author manages the generating of the pair of keys from the cryptomodul possessed by him.

5. Procedures for providing certification services by SEP Bulgaria

SEP Bulgaria provides to its Client s certification services on issuing and management of Certificates for QES at strict observation of the stated below rules and procedures.

Each procedure starts with submission of the relevant Request by the Author/Holder or by a person with explicit power of attorney for the procedure. The submitted demand contains data for the relevant service and needful information for identification/authentication of the Author/Holder and relevant declarations for referent facts and rights.

5.1. Submission of requests

The request for the relevant service is submitted:

- To operator of RA.
- To SEP Bulgaria through the electronic page of SEP Bulgaria;

The requests are submitted in electronic form or in written form.

5.1.1. Requests in written form

The requests in written form are submitted to RA by some of the following ways:

- Personally to operator of RA ;
- By indirect method giving the same level of security - the same as with personal submission.

In case of necessity depending on the relevant procedure RA demands introduction of the additional data and documents for applying for certification service.

5.1.2. Requests in electronic form

The requests in electronic form are submitted through the electronic page of SEP Bulgaria by following the instructions for each step of the process.

For submitting requests by electronic way through the electronic page of SEP Bulgaria are used network protocols like HTTPS, S/MIMME or TCP/IP.

In case of necessity depending on the relevant procedure is pointed RA before whom will be introduced additional data and documents (accompanying the request documents), needful for receiving of the requested certification service.The accompanying the request documents may be submitted in an electronic way together with the specific request so in this case there is a regulation for the documents to be legalized by the notary.

The request is processed by the operator of RA by check and comparison the data from the submitted request with data from other resources and additionally introduced data and documents for receiving certification services upon the order of section VII of this Chapter.

5.2. Processing the requests of RA

The requests are processed by Operator of RA in a following way:

- The operator checks the data indicated in the Request and when it`s applicable checks the proofs concerning the hold of private key by the Author;
- The data are being verified with data from public registers and/or additionally granted documents;

- RA may check and other data when it is necessary;
- In case of successful check, the Operator approves the request by signing it. At wrong and incorrect data the Request is denied;
- On the basis of the approved Request an electronic application is submitted to the CA through the specialized software as the operator of RA guarantees the correspondence between the data in the electronic application to CA with the data, containing in the particular request.

RA makes up and passes to CSP the gathered documents meaning the requested by the Client certification service on issuing and management of certificate for QES.

5.3. Processing the applications by the CA

CA proceeds the received upon the order of p 5.2. from this section electronic applications by the following way:

- Checks if the application is received by RA with power of attorney and makes authentication of the operator of RA submitted the particular application;
- Connects the data from the Request with the available data for Author/Holder from his base with data;
- Leads records for processing in the base with data the systematic books of PKI and the Register.

5.4. Procedure of issuing a certificate for QES

Issuing a new Certificate for QES represents an entry of the relevant Certificate in the „List of the issued certificates" in the public electronic register of CSP.

The issuing is accomplished on the basis of submitted Request for issuing a Certificate for QES. The information which is fulfilled in the request must be comprehensive and tangible depending on the type requested Certificate for QES. The information upon the preceding sentence includes:

- The full name of the Author, and also his pseudonym, if there's is a request for entry of such in the relevant certificate;
- Full name of the Holder ;
- Full name of the person having the power of attorney to represent the Holder /Author at application of the service (applicant);
- Identificators of the Author: UCN, IDN, number of ID, date of issuing and validity of the document, body – publisher of the identification document;
- Identificators of the Holder: UIC, IN to VAT
- Identificators of the applicant: UCN, IDN
- Permanent address/ residence and address of administration of the Holder y;
- Permanent/office address of the Author;
- Type of applied Certificate for QES;
- Electronic address of the Author for the purposes of usage the Certificate for QES;
- Additional information, needful for getting a of the required type of Certificate for QES;
- Data for the representation power of the Author – sort, number and date of the document certifying the representation power, marks of individualization of the body issued/certified the document.
- Data and information for the affiliation to the relevant branch/profession`s organization.

Together with the delivery of the stated above information the person issuing the Request for issuing a Certificate for QES, should introduce the following declarations about:

- Fullness, propriety and accuracy of the introduced with the Request data;
- The preservation and processing of the personal data containing in the Request;

- The availability or the lack of desire for restraining the public access to the required Certificate for QES.

At receiving a Request for issuing a Certificate for QES, CSP through particular RA:

- Accomplishes the particular identification/authentication of the person upon the order section VII, т. 1 of this chapter;
- Processes the Request upon the order of point 5.2. of this section;
- Cincludes a contract certification services (if the particular contract is binded with tangible certificate);
- Issues an invoice for the tax paid:
- RA submits electronic application upon the order of p. 5.3 from this section to the server of CA for issuing a Certificate for QES in according to the provisions:
  - The algorithms for check of Certificates of QES to constitute a logical whole with algorithms for their creation;
  - The algorithms and the parameters for qualified electronic signature to respond to particular provisions regarding the hash-functions and the asymmetrical algorithms according to the provisions of ORACCQES;
- If the procedure is successful, the server generates the Certificate and signs it by using hardware crypto module. The generated certificate is preserved in the base of data of CA and is published in the public electronic register of CA;
- CA prepares an answer containing the generated certificate for QES and introduces it to the Client by RA or by electronic way.

The issued Certificate for QES is considered valid from the moment of its publication in the public electronic register of CSP.

The publication of the Certificate for QES in the Register is equivalent to informing the Relying parties for the fact that a certificate of the person has been issued, entered in it and this person may be identified through this QES.

5.4.1. Denial for issuing a Certificate for QES

CSP has the right to deny issuing a Certificate for QES in the following cases:

- The Author/Holder hasn`t introduced the eligible documents for issuing a certificate for QES;
- The applicant cannot prove the availability of explicit representative power concerning the factual material and the legal actions on delivery with Certificate for QES;
- When there are doubts that on conducting of the procedure of issuing a Certificate for QES are used false data and/or unauthentic or forged document;
- In case of not responding to the provisions of art.25, par.2, p.3 from EDESEA
- It has been reached a preliminary negotiated limit for number of issued Certificates for QES of a particular Holder/Author;
- At availability of other grounds for denial regulated in the proactive legislation.

The information for denial for issuing of Certificate for QES and the reasons related to that are announced to the applicant. The person who is rejected the Certificate for QES can submit litigation in the terms of 3 (three) days upon the order, provided in Chapter First, section VI.

5.4.2. Acceptance of the content of the issued Certificate for QES

The Author/Holder can reply, if the issued Certificate contains mistakes or incompleteness in terms of 3 (three) days from the publication in the public electronic register of CSP.

CSP issues a new Certificate for QES without additional payment except in the cases when the mistakes are a consequence of submitting of false data by the Author/Holder or the person with power of attorney.

In case that the Author/Holder doesn`t submit litigation in the above stated term is considered that the containment of the issued Certificate is accepted.

5.5. Procedure for the renewal of Certificate for QES

The renewal of valid certificate for QES is issuing a new Certificate for QES declared before the expiration of the term of the action of the valid Certificate for QES. There is renewal only for valid certificates, which are not terminated and information in them is not changed.

The renewal is committed by declaration of Request for issuing a Certificate for QES on the grounds of renewal. The information which is fulfilled in the request should contain identical information to those submitted by the person at the Demand for issuing of the renewed Certificate as it is stated in p.5.4 of this chapter.

When receiving a Request for renewal of certificate for QES, CSP through relevant RA:

- Accomplishes the relevant identification/authentication of the person under the order of section VII, p. 1;
- RA proceeds the Request by the order of p.5.2 of this section;
- Concludes a contract for certifications vices (if the relevant contract is binded with tangible certificate);
- Issues an invoice for the paid tax;
- RA issues an electronic application under the order of p.5.3 of this section to the server of CA for issuing a certificate for QES;
- If the procedure is successful server generates the certificate and signs it by using a hardware cryptomodul. The new certification for QES is with new serial number and terms of action. The generated certificate is preserved in the base of data of CA and is published in the public electronic register of CA;
- CA prepares an answer containing the generated renewed certificate for QES and introduces to the Client by RA or by electronic way.

SEP Bulgaria publishes information for the renewed Certificate for QES in its public electronic register. The publication of information for the Certificate for QES is equal to notification of the Relying parties for the fact that the person, entered in it owns valid Certificate and may be identified through the relevant QES.

SEP Bulgaria has the right to deny the renewal of a Certificate for QES in the sense of hypotheses from p.5.4.1 of this section – as stated above.

The Author/Holder may reply, if the issued and renewed certificate contains mistakes or incompleteness in terms of 3 (three) days from the publication in the public electronic register of CSP.

CSP issues a new certificate for QES without additional payment except in the cases when the mistakes are a result of submission of false data by the Author/Holder or the person with power of attorney.

In case that Author/Holder doesn`t submit a reply in the term stated above is considered that the contents of the issued renewed Certificate is accepted.

5.6. Procedure for modification of certificate for QES

Modification of certificate for QES is an issue of a new certificate on the grounds of issued before this valid certificate at change of information, entered in the Certificate.

The range of the admissible change is an entry of new contents or insertion of new information.

There is modification only of valid certificates which are not terminated.

The modification is done by submitting a Request for issuing a certificate for QES on the grounds of modification. The information which is inserted in the demand must contain the information, submitted by the person at the preceding demand for issuing a certificate as it is stated in в p.4 from this section and the relevant new content from the admissible range.

The Request is submitted to CSP under the order provided in p. 5.1 from this section.

At receiving of request for modification of certificate for QES, CSP:

- Accomplishes the relevant identification/authentication of the person under the section VII, p.5.1.2;
- RA proceeds the demand by the order of p.5.2 of this section;
- Concludes a contract for certification services (if the relevant contract is binded with tangible Certificate);
- Issues invoice for tax paid;
- RA issues electronic application to CA for issuing a certificate for QES upon the order of p. 5.3 form this section;
- The manipulated, upon the order of p. 5.3 from this section electronic, application is transferred to the server of CA for issuing a Certificate;
- If the procedure is successful the server generates the Certificate and signs it like using a hardware crypto module. The new certificate for QES is with new serial number and term of action. The generated certificate is preserved in the data base of CA and is published in the public electronic register of CA and the modificated Certificate is terminated;
- CA prepares an answer containing the generated new Certificate for QES and gives it to the Client CA or by electronic way.

SEP Bulgaria publishes information for the modified certification for QES in the public electronic register. The publication of the information for the Certificate for QES is equal to information of the relying parties for the fact that the person entered in it has a valid certificate and may have an authentication by the relevant QES.

The modified certificate for QES is revoked with reason for termination affiliationChanged. This is the way to show that the Certificate is replaced by another with modified data and informs the relying parties that the private key relevant to the public from the replaced Certificate hasn`t been discredited.

SEP Bulgaria has the right to deny the modification of certificate for QES in the above stated in p.5.4.1.of this Section hypotheses.

The Author/Holder may reply if the issued during the procedure of modification new Certificate contain mistakes or incompleteness in the terms of 3 (three) days from the publication in the public electronic register of CSP.

CSP issues a new certificate for QES without additional payment except in the cases when the mistakes a result of submission of false data by the Author/Holder or by the person with power of attorney.

In case that the Author/Holder doesn`t reply in the terms stated above it is considered, that the contents of the issued modified certificate is accepted.

5.7. Procedure of suspension of Certificate for QES

The suspension of Certificate for QES is a temporarily inclusion of the certificate in „ the List of revoked certificates". For the time of the suspension of the certificate, the certificate is considered invalid and all electronic signatures authenticated with this Certificate are invalid.

The action of a valid Certificate may be suspended on the certain grounds for the terms according to the circumstances but not for more than 48 hours.

Suspension of the certificate for QES happens in the following case:

- On a Request submitted to CSP by the Author or Holder or by the person with power of attorney, without CSP to have the obligation to be assured in his identity or his representative power;
- On request of a person for which the circumstances show that he might know for RA each of security of the private key, as a representative,associate, personnel, member of the family and so on.;
- On request of the Communications Regulation Commission;
- By decision of the chairman of the Communications Regulation Commission.

The request for suspension (being a type of Request for management) is submitted to CSP upon the order provided in p.5.1 на of this section and it is supposed to contain and information for the reason of suspension.

When receiving a request for suspension of the Certificate for QES, CSP processes it by the following order:

- RA processes the Request by the order, provided in p.5.2 from this section.
- RA submits electronic application to CA for the suspension of QES on the order of p.5.3 of this section;
- CA checks the validity of the Certificate which suspension is asked and the correspondence between the data in the demand and the data entered in the Certificate;
- CA suspends the action of the Certificate by inserting in it in „List of suspended certificates“ with a reason for suspension „hold“;
- CA in an instance informs the Holder/Author for the suspension of the action of the certificate.

SEP Bulgaria publishes information for the suspended certificate for QES in his public electronic register.The publication of the information for the Certificate for QES is equivalent of informing the relying parties for the fact that the relevant Certificate is not valid and the person entered in it cannot have authentication through the relevant QES.

5.8. Procedure for reactivation a certificate for QES

A reactivation of Certificate for QES is an exclusion of the Certificate from the „List of revoked certificates“. After the reactivation of the Certificate the last one is considered valid.

The reactivation of suspended Certificate is accomplished in the following cases:

- After expiration of the maximum term for suspension of 48 hours – automatically;
- Before the expiration of the maximum term of suspension – by the deliverer of certification services – at declining of the grounds for suspension or by Request of the Author or Holder, after CSP and respectively the Communications Regulation Commission has been assured that he has known the reason for the suspension and the Demand for renewal is made a s a consequence of the fact of knowing the reason.

The request for reactivation (which is a type of Request for management) by the Author/Holder is submitted to CSP upon the order provided in p.5.1 of this section.

The information which is containing in the Request is the following one:

- Information for the reactivated certificate;
- The full name of the Author;
- The full name of the Holder;
- The full name of the person having the power of attorney to represent the Holder /Author at declaring of the service;
- Identificators of the Author/Holder: UCN, IDN, UIC,;
- Permanent address/residence and address of administration of the Holder;
- Permanent/office address of the Author;

- Reason for reactivation;
- Declaration that the Author/Holder has known the reason for the suspension and the Request for reactivation is made as a consequence of the fact of knowing the reason.

At receiving a Request for reactivation a certificate for QES by the Author/Holder, CSP processes it in the following order:

- Accomplishes the relevant identification/authentication of the person upon the order of section VII, p.5.2;
- RA processes the Demand upon the order of p. 5.2 of this section;
- RA submits electronic application to CA for the renewal of Certificate for QES upon the order of p.5.3 from this section;
- CA checks the validity of the Certificate which renewal is required and the availability of grounds for the demand and the correspondence between the data in the Request and the data, entered in the Certificate;
- CA reactivates the suspended Certificate but excluding it from the „List of the suspended Certificates";
- CA in instance informs the Holder /Author for the reactivating of the action of the certificate.

CA reactivates a suspended Certificate after getting of written direction from the Communications' Regulation Commission or from the chairman of the Communications Regulation Commission for reactivation or in an instance after the expiration of the maximum period for suspension (48 hours).

From the moment of reactivation of the Certificate the same is considered valid. SEP Bulgaria publishes information for the renewed certificate for QES in its public electronic register. The publication of the information for the Certificate for QES is equivalent to information of the relying parties about the fact that the person, entered in it owns a valid Certificate and may have an authentication through the relevant QES.

5.9. Procedure for revocation of QES

Revocation/termination of certificate for QES is an insertion of the Certificate in the „List of revoked certificates"(CRL). From the moment of the insertion of the Certificate in the CRL last one is considered invalid and all the electronic signatures having an authentication by this Certificate are invalid.

Revocation of the Certificate could happen in the following cases:

- Death or putting the Author under judicial disability;
- Suspension of the representative power of the Author regarding the Holder , when the certificate is issued with an entry of the Holder ;
- The suspension of the juridical person of the Holder when the certificate is issued with entry of the Holder;
- Determination that the Certificate issuede on the basis of false data;
- Discredit (or doubts for discredit) of the private key responding to the public key from the Certificate or the bearer used for its preservation;
- Demand of the Holder or the Author for suspension of the Certificate and/or for termination of the contract with SEP Bulgaria issued upon the order of p.5.1 of this section;
- At discredit of the private key of CSP;
- At non-performance (full or partial) of obligation for payment of the definite taxes for the usage of the certification services;
- At termination of the activity of CSP. In this case are suspended all the issued Certificates, and the certificates of CSP as well;
- At non-performance by the Holder/Author of his obligations according to this Guide or cincluded contract for certification services;
- With the expiration of the terms of action of the Certificate;

- The request for revocation is issued by the same way:
- By the Holder/Author or person with explicit power of attorney;
- By the demands of bodies indicated in a normative act.

When the revocation is made by request of the Author/Holder, the Request for revocation (being a type of Request for management) is submitted to CSP upon the order provided in. p.5.1 for this section.

The information which is containing in the Request for revocation is the following:

- Information for the revoked Certificate;
- The full name of the Author;
- The full name of the Holder ;
- Full name of the person having the power of attorney to represent the Holder /Author at declaration of the service ;
- Identificators of Author/Holder : UCN, IDN, UIC;
- Permanent address/residence and administrative address of the Holder ;
- Permanent/office address of the Author;
- Reason for revocation.

When receiving a Request for revocation a Certificate for QES, CSP processes it by the following order:

- RA makes an identification/authentication of the Author/Holder upon the order of section VII;
- RA processes the Request upon order, provided in p.5.2 of this section;
- CA processes the Request upon the order provided in p.5.3 of this section;
- CA publishes information for the revocation of the Certificate in CRL together with information about the reason for revocation;
- CA sends confirmation for suspension of the Certificate to the applicant of the Request for revocation;
- CA in instance informs the Holder /Author for the revocation of the action of the Certificate.

SEP Bulgaria publishes information for the revoked Certificate for QES in the public electronic register. The publication of the certificate for QES in the CRL is equal to information of the Relying parties for the fact the Certificate is not valid and the person, entered in it, cannot have authentication through the relevant QES.

5.10. Maintenance of Certificate for QES

The maintenance of certificate for QES is the providing of possibility of usage of the following services for a definite period in the terms of action of an issued valid certificate:

- Services of management (suspension, reactivation and revocation) of issued valid certificate for QES;
- Services for Time stamp of introduction of QES created for definite electronic document;
- Services for publication of topical information for the Certificate for QES in the public electronic register of CSP according to the Request of the Client ;
- Services of validation – making a check of the validity of the issued Certificate by the Relying parties.

Only valid certificates are maintained, which are not revoked and the information containing in them hasn`t been changed.

Considering the fact of accomplishing of annual maintenance during the period of validity of the Certificate, the Client submits a Request for maintenance. The request for maintenance should be submitted till the end of the relevant annual period.

The information which contains in the Request is the following:

- Information for the supported Certificate;

- Full name of the Author;
- Full name of the Holder ;
- Full name of the person having the power of attorney to represent the Holder /Author at declaration of the service;
- Identificators of the Author/Holder: UCN, IDN,UIC;
- Permanent address/ residence and administrative address of the Holder ;
- Permanent/office address of the Author;
- Declaration on unchanged data.

The demand is submitted to CSP upon the order provided in p. 5.1 of this section.

At receiving a Request for maintenance of Certificate for QES, CSP:

- Makes the relevant identification/authentication of the person on the order of section VII;;
- Issues an invoice for the paid tax;
- Processes the demand for maintenance of certificate for QES upon the order of p.5.2 this section.

In case that the Client does not submit Demand for maintenance of certificate for QES in the provided for this term, the certificate will be suspended.

6. Usage of the Certificate and the key pair

The Holder /Author may use the private key and the Certificate for QES:

- According to its function, as it is indicated in this document and it is relevant to the contents of the Certificate for QES (fields keyUsage, EnhancedKeyUsage);
- According to the Contract for certification services concluded between them and SEP Bulgaria;
- In the terms of validity of the Certificate unless for the purposes of documents decryption and check of the electronic signature;
- Until the suspension of the certificate for QES;
- When the Certificate is suspended and the Holder /Author have used the private key for putting an electronic signature, the signatures will be considered veritable only if the Certificate is renewed.

The Relying parties can use public key and the Certificate for QES:

- According to their function as it is stated in this document and according to the contents of the certificate for QES (fields keyUsage, enchansedKeyUsage);
- Only to check the status of the issued Certificate for QES and check of the electronic signature;
- Until the moment of suspension for public keys for key exchange, data encryption *или* key agreement;
- When the certificate is suspended, the Relying party should not use the public key from this Certificate.

7. Necessity of the check of the status of the Certificate for QES

The responsibility of the Relying parties, at receiving a document signed with QES is to check if the public key for the Certificate, which responds to the private key of the Author used at the electronic signature is not published in CRL. The relying party should make the check online in the current CRL or by OCSP.

If the checked certificate for QES (respectively public key is included in CRL, the Relying party should deny the document associated with the Certificate if the reason for inclusion in CRL is one of the following:

Reason	**Definition**
Unspecified	There is no specified reason for inclusion the certificate in CRL

keyCompromise	The security of the private key is breached
caCompromiced	The security of the CA is breached
cessationOfOperation	The grounds for issuing a Certificate doesn't exist anymore
certificateHold	The certificate is suspended
affiliationChanged	There is modification of the data entered in the Certificate
Superseded	The certificate has been superseded with another certificate

The ultimate decision about the acceptance of the validity of the Certificate is taken by the Relying party. CSP doesn`t take responsibilities for the actions of the relying party at non-performance of the stated above provisions.

7.1. Online check of the validity of Certificate for QES

SEP Bulgaria gives the opportunity for check in real time, online, the status of the issued Certificates for QES. This service is provided through OCSP protocol described in RFC 2560. The model of delivery of OCSP service is based on the process „answer-respond". The answers, which are received by OCSP server ensuring the service, are the following:

Answer	**Meaning**
good	The certificate is valid
revoked	The certificate is revoked
unknown	The status of the certificate is not identified or the certificate is not issued by the relevant CA.

7.2. Services of validation

The Relying parties can change the status of the issued by SEP Bulgaria certificate for QES by one of the following ways:

- In the CRL published in the public electronic register of SEP Bulgaria;
- By OCSP protocol.

The needful actions for accomplishing the check are:

- Pulling out CRL and installation in the application of the relying party. The electronic address from which a CRL can be pulled out is indicated in each issued Certificate;
- AT OCSP – sending an application for validation to the server of SEP Bulgaria. Protocol for exchange is defined in RFC 2560.

7.3. Availability of the service

The service for validation is available 24 hours 7 days in the week. In case of accidents and natural disasters, SEP Bulgaria takes immediate measures to restore the service for validation.

8. Issuing a certificate for time

SEP Bulgaria issues a certificate for time at introduction of electronic signature created for definite electronic document.

The certificate for time has official power of certification after its entry in the Register of CSP for the issued certificates for time.

The system of SEP Bulgaria for certification of time accepts appeals according to IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol.

8.1. Procedure for certification of time

The system of SEP Bulgaria, ensuring the Certificate of time accepts applications and returns answers in format defined by RFC 3161 - „Internet X.509 Public Key Infrastructure - Time-Stamp Protocol".

In the application it is necessary to have containing of hash of the electronic signature of the document which time of setting is certified and version of the application.

The application for certification of time is sent to electronic address: http://tsa.sep.bg and can be generated by special Client `s software.

The in-coming applications are processed consecutively. The accuracy with which the certificates for time are issued by SEP-Bulgaria is one second. The certificate of time contains the following elements:

- Status;
- Version of certificate for time;
- Identificator of the certified document;
- Consecutive unique serial number;
- Time of signature by ZULU;
- Identification of the deliverer of certified time – SEP Bulgaria.

The certificates for time are signed with private key designed only for this activity.

9. Termination of the usage of certification services

SEP Bulgaria does not have engagement to the Holder regarding the delivery of services about management of Certificates for QES after the contract concluded between them is terminated or expired.

The Client of certification services of SEP Bulgaria can terminate at any time the usage of the certification services.

On demand of termination of the usage of the certification services, SEP Bulgaria terminates the contractual relations with the Holder/Author and terminates the issued Certificates in which the Holder /Author is entered.

SEP Bulgaria does not compensate the Holder/Author at termination of the usage of the certification services on his demand.

VIII. Equipment, leadership and operational controls

In this section are introduced the General rules considering the management of CSP and accomplished controls regarding the physical and organizational security and the activities of the staff at delivery of certification services by SEP Bulgaria.

1. Equipment of the Provider

1.1. Physical security at CA

The network computer systems, the terminals of the operators and the information resources of SEP Bulgaria are situated in detached places – physically protected against unauthorized access, demolition and interruption of the operations. These places are observed and guarded day and night. There are records of each entering and leaving in a book. There is observation of the indicators of the electricity supplies, temperature and humidity of air.

SEP Bulgaria has premises with relevant degree of physical protection against violation. The premises are with climatic conditions, with controlled physical access provided basic and stand –by electric supply, provided basic and stand-by communicational channel.

1.1.1. Physical access

The building is guarded by 24 hours physical guards. A technical system is constructed observing for violation to the territory of the building and to protected premises.The adjoining territory and premises are 24 hours video observation.

The physical access is observed and controlled by integrated system for security observing for the presence or absence of staff in the premises of CSP.

There is a fire-alarm system and measures have been taken against flooding the premises.

The systems are ensured against declination of the power supply of the premises; measures have been taken against occasional interruptions and hesitations in the power supply network (UPS) and against long term interruptions of the power supply (generator).

Depending on the activities proceeding in the relevant premises – part of them is publicly available and the access to others is controlled or possible only for authorized personnel. For definite premises there is a requirement of two authorized people from the staff simultaneously.

Visitors and auditors are permitted access if they are accompanied by staff of SEP Bulgaria, having the right to access the visited premise.

All the staff and visitors are wearing badge with information for the physical access zone and the regime for access.

The protected areas are equipped with systems for physical control and observation and fire-alarm systems and fire extinguishing systems. Access to these zones has only authorized staff from SEP Bulgaria. Entering and leaving the zones and the movement in premises from the zones is tracked down and recorded by system of control of access. The companions may pass only after confirmation by authorized staff.

1.1.2. Electric supplies and air-conditioning

When there is failure in the main supply the systems switch to stand – by supply.

When there is short failure and hesitation and UPS is used. In case of prolonging failure a generator is switched on.

All premises are with fans and air-conditioning. The ventilation is designed and built is a way not to compromise the physical security of the premise.

1.1.3. Flood

Measures have been taken for preventing the flooding of the premises of SEP Bulgaria. There is a procedure to reacting to problems connected with Acts of God or industry damage.

1.1.4. Fire precautions

Measures has been taken for discovery and putting out fire in the premises used for the activity of SEP Bulgaria.There is a procedure for action in matter of fire. All premises depending of their type are equipped with resources for putting out fire according to the normative provisions. In the protected premises and archives is built up an automatic system which switches on automatically at discovering fire.

1.1.5. Preservation on bearers

Depending on the sensitivity of the preserved on the bearer's information, the bearers with archives and reserve copies ate preserved in fireproof safes situated in the protected premises. The access to the safes is accomplished through keys holder by authorized staff. Copies of this information are preserved at the same conditions outside of the major premises.

The bearers used for archives of the current information and reserve copies and the paper documents are preserved in safes situated to CSP. The period of preservation is 10 (ten) years from receiving the information and conclusion a contract with the Client.

1.1.6. Trash

Paper and electronic bearers with sensitive data after expiration of the period for storage are destroyed in proper way so to become impossible to know the information on them.

1.1.7. Storage of the reserve copies

SEP Bulgaria preserves reserve copies of all needful data with which help may recover its operations in the terms of 48 hours. These are copies of the actual data and reserve copies of the informational systems.

1.2. Equipment of RA

The computer systems in RA are situated in equipped premises and work in online regime- on accepting and processing the demands of the Client s. The access is physically restrained. Measures taken ensuring systems to be used by authorized persons.

Actual list with addresses of the acting bodies of registration is published at the electronic page of SEP Bulgaria.

1.2.1. Security of the Holder /Author

The Holder /Author are responsible for the preservation and keeping the secret of the passwords for access, identification codes, PIN and deblocking PIN.

1.2.2. Control of the procedures

All the procedures are accomplished according to EDESA, the provisional documents developed by CSP and the internal procedures and rules by staff and according to delegated rights and obligations.

2. Leadership and staff

2.1. Trusted positions

SEP Bulgaria makes characteristics of positions according to section IV of „Ordinance for the activity of the providers of certification services, the order of their termination and the provisions for providing of certification services".

CSP has got in its organizational structure different positions for the execution of the following activities:

- Generating and maintaining the infrastructure of the public key of CSP;
- Management and providing security of the systems;
- Creation and management of corticated for qualified electronic signature including the creation of pair of keys – private and public – for qualified electronic signature;
- Preservation of data and archives.

2.2. Management of the personnel

SEP Bulgaria is taking measures to guarantee a high level of the personnel during the execution of obligations of providing certification cervices. The measures on employment are the following:

- The persons have graduated secondary school minimum (unless something else is required for the position);
- Introducing a certificate showing on previous conviction;
- Concluding an employment agreement with applied characteristics for the position, describing the obligations and the responsibilities;
- Signing a declaration for confidentiality;
- Passing an educational course for the position;
- Having instructions of work with Client s and protection of personal data.

2.3. Qualification and experience

SEP Bulgaria appoints at the relevant positions persons who have knowledge's in the following areas:

- Security technologies, cryptography, public codes infrastructure (PCI);
- Ttechnical standards for evaluation of the security;
- Information systems.

Before hiring someone to the respective job positions, SEP Bulgaria validates his knowledge and qualifications.

2.4. Training of the personnel

The personnel of the deliverer of the certification services – SEP Bulgaria is having training in the following fields:

- Regulation related to EDESA and the subordinate acts on its application;
- Regulation related to „Policy for delivery of the certification services";
- Regulation related to „Practice for delivery of the certification services";
- Regulation related to internal procedures and documents for the relevant position;
- Procedures and controls related to the information security;
- System software of CA and RA ;
- Customer service and protection of personal data.

The training of the staff is repeated:

- On necessity of confirmation of the knowledge and skills related to execution of the obligations for the position;
- Through certain periods of time;

- At substantial changes in the provisional documents;
- On necessity of analysis of critical situation or incident.

2.5. Disciplinary measures

When there is non-performance of the obligations for the relevant position SEP Bulgaria applies disciplinary sanctions depending on the type and the extent of the violation and also according to relevant labor legislation.

2.6. Contracts with outside persons

On concluding contracts with outside persons (outside services, development of software and so on.) they are subject to the same procedures as the staff of its own.

2.7. Documents given to the staff

The leadership of SEP Bulgaria, gives access to the staff from CA and RA to the following documents:

- EDESA and the subordinate acts on its application;
- „Policy for providing certification services";
- „Practice on delivery of certification services";
- Forms of requests and patterns for all types of used documents;
- Internal procedures and documents for the relevant position;
- The procedures and controls related to the information security;
- Guidance for the usage of the system software of CA and RA ;
- Procedures for auctions on extreme situations, damages, failures and Acts of God.

IX. Leading of the records and check of the books

For effective control on the activities and staff, SEP Bulgaria leads records on all the activities having influence on the security.

As a matter of obligation each group or team, related to the provision of certification services, leads records for its activity and is responsible for their management according to the position and the obligations the group has.

The information records from each book are preserved and are a subject of access only by authorized persons for getting of information needful for arguing of disputes or for discovery and tracking down of information security breaches. All the records ate put into archives. The archive copies are preserved outside of the major premises in CSP.

The generating of records in the books happens automatically. If it is impossible the events are recorded on a paper bearer. All the records – automatic and on paper are granted when there are checks of the activity of CSP.

Manager IT Security is obliged to make regular checks for correspondence of the accomplished mechanisms and procedures to the relevant legislation and this practice and to appreciate the effectiveness of the existing procedures on the security.

1. Type of the events recorded

Each critical activity regarding the security of SEP Bulgaria is recorded in a book and is put in an archive. The archives may be encrypted and preserved on bearers for electronic signature in order to prevent their theft or modification.

All the books generated, generated by the software components of the information system of Sep Bulgaria ate preserved. The records are divided in a few categories:

- System recordings – the recordings contain information about the system events;
- Recordings for mistakes – the recordings contain information about the mistakes on the level of protocol and application;
- Recordings from observation – the recordings contain information related to the certification services like issuing of demands for creation of certificates, acceptance of certificates, issuing of certificates and list with suspended certificates.

Each recording no matter on a paper or automatically generated contains the following information:

- Type of the event;
- Identifier of the event;
- Date and hour of the event;
- Identifier or other data which allow to have an identification of the person, responsible for the event;
- The decision which responds to successful or wrong operation.

The records can be:

- Alarms from fire walls and network sensors;
- Operations responding to registration, certification/issuing, change of keys and renewal, suspension, stopping/renewal or other services delivered by CA;
- Each change of software of hardware;
- Physical visit of the protected parameters and violation of the protected parameters;
- Change of PIN, passwords and rights for the access of the personnel;
- Successful and unsuccessful attempts for access to data base of CSP;
- GENERATION of keys for CA and other elements from the infrastructure for providing of certification services;
- Each received demand in electronic form;
- All the correspondence in electronic form between CSP and the other participants in the certification services;
- History of the archive copies of the books, system and data bases.

Access to the books have only managers IT security and persons making check of the activity of CSP.

2. Review of the books

One a month there is a review of the books including for their integrity and authenticity. Once a week the books are reviewed by a randomly chosen operation.

At accident or doubt for accident on security all the books files are being checked.

3. Period of storage

The books are preserved on the discs of the information systems until a certain rate is reached. During this time they are available online for all the authorized personnel.

At the reach of certain rate, the books are transformed in archives. The archives are kept at least 10 (ten) years from the receiving of the information and conclusion a contract with the Client .

4. Protection of the book files

The book files are encrypted for archiving the key for the archives is under the exclusive control of Manager IT Security.

The book files can be reviewed only by authorized staff and persons who have the obligation to make review and analysis of the files. The access to the book files is structured in a way giving the opportunity:

- Only authorized staff – persons making a check and personnel of CSP, to have the right to review the books;
- Only manager IT Security has the right to put to archive and erase files containing the registered events;
- Discovery of each violation of the integrity of the data and a guarantee that each record is authentic (not forged).

Nobody has the right to modify the contents of the book files.

The above stated rights for access are relevant for records which has been put to archives and handed over for storage.

5. Putting to archives the book files

SEP Bulgaria once in a month put to archives the books for events and the records for activities on their review, analysis and statistics, evident treats and measures taken. The archives are kept in the major and far away office of SEP Bulgaria. The archive copies which are in electronic form may have certified time of their creation.

X. Notification for events

SEP Bulgaria runs an observation and analysis of the system events so when there is a suspectful event the responsible persons are being notified.

The notified persons take the relevant actions for protection of the system depending on the treat.

XI. Evaluation of the vulnerabilities

SEP Bulgaria in its capacity as CSP and all the persons delivering certification services on his behalf and on his account periodically make evaluation of the vulnerabilities through analyzing the internal procedures, applications and the information systems.

XII. Putting the records to archives

All data and files related to the registration of the users of the certification services and the security of the systems, the information granted by the Holder /Author, the issued certificates, the generated CRL, the keys used by RA and all the correspondence between SEP Bulgaria and Holder /Author or authorized representatives are put to archives. The following documents are being put to archives: the documents and the data used for identification of the Holder/Author and check of identity respectively the identity of Holder/Author.

The documents introduced in written form when it is possible ate transformed in electronic form and being put to archives.

SEP Bulgaria maintains electronic and paper archives.The archive is preserved for the period of 10 years.

1. Types of archival data

The following data are being put to archives:

- The information from the checks and evaluation of the logic and physical protection of the CA and RA and the public electronic register;
- Data base with the users of certification services;
- Data base with certificates;
- The generated CRL;

- History of management of the keys of the CA of CSP;
- History of the user`s keys, generation, providing, distraction of the archive copies after their providing to the author;
- Internal and external correspondence in written and electronic form between SEP Bulgaria and the users of the certification services and RA ;
- Documents and data used in the process of the check of identity respectively the identity of the Holder /Author.

2. Frequency of putting to archives

Data are being put to archives on different levels according to the following time schedule:

- Data base with user`s certificates and the data of the Holder/Author are preserved on the servers of Sep Bulgaria up to 10 (ten) from the moment of the issuing of the certificate or the last action on its management and archived on a visual bearer without possibility for addition or erasing of records.
- The bearers with the data are transferred to documental archives for storage.

The list with the suspended certificates, the correspondence and the applied demands, as well as the decisions taken, are preserved according to the above stated scheme.

3. Periods of storage in archive

The archived data in written or electronic form are preserved for period of at least 10 (ten) years. After the expiration of the definite period, the archived data are being erased. At demolition of keys and certificates are applied the respective procedures.

4. Protection of the archive

Sep Bulgaria establishes resources and takes measures allowing maintaining the integrity and the availability of the data form the archive. The measures include the following basic rules:

- Only authorized personnel on trusted positions has the right to access to the archive;
- The archive is protected by modification, the records are signed with electronic signature and the data are archived on bearers for one way record запис;
- There is maintenance of more than one copy on different, physically protected places with purpose protection form destruction of the archive;
- In order to protect an archive from damages because of the aging of the bearers which it has been recorded on, the archive is periodically transferred to new bearers and the old ones are being destroyed. There is periodical change of the bearers on which the daily archives are made;
- The form of the data and the bearers on which is being recorded or transferred a record of the archive is changed if there is a necessity in order to be protected because of the impossibility to use because of change of the technologies, the algorithms, the formatting of the data and the hardware for archiving;
- Resources are being maintained for the access to archives created in past period of time.

5. Reserve copies of the archive - procedure

The reserve copies allow the full recovery in the case of necessity of the major data, needful for the right functioning of CSP. In order to have this purpose achieved reserve copy is made of the following data and files:

- Installation discs with system applications;
- Installation discs with the applications of CA and RA ;
- WWW server and the discs with installation of the public electronic register;

- The data from the public electronic register, data base with users of certification services and system data base;
- Other data related to the activity of SEP Bulgaria ,as CSP;
- The book files.

The methods of creation of reserve copies used by SEP Bulgaria are:

- Daily reserve copies – each day reserve copies are made of the data base and may be used for the recovery of lost data;
- Weekly reserve copies – they are used for recovery of the system at damaging the hardware or at necessity of recovery of the settings of the system software to definite moment of time. These copies reflect the current state of the information systems.

SEP Bulgaria can recover its systems entirely in the terms of 48 hours.

Detailed description of the data and the procedures by which the reserve copies are made is a part of the documents for the technical infrastructure of CSP. These documents do not have public characters and are available exclusively for the authorized personnel and persons checking the activities of SEP Bulgaria.

6. Request for the certified time for the records

When having a possibility a certain time is certified for all the archival data regarding the time they have been created to.

7. Procedure for check of the archived information

In order to check the integrity of the archived information, the data are being periodically tested and checked and collated with the original data if they are still available in the operative information systems.

This activity is accomplished only by authorized personnel and is reflected in the book of the system.

In case there is damage in the data immediate steps are taken for the recovery of the integrity of the archive.

XIII. Change of keys

CA of SEP Bulgaria changes the keys with which signs the issued certificates and list of suspended certificate by sticking to the following procedure:

- A special certificate by CA is issued – for the users, who own the old certificate of CA with which is guaranteed the protected exchange of the new certificate. By this way the new users are allowed to get in secure way the old certificate for the purpose of the check.
- Each change of the keys is preliminary declared on the site of CSP, the CRC is informed and all the Holder/Author is informed.
- The regularity of the change of keys is defined by the period of validity of the certificates of the basic and operational CA.

From the moment of the change of the key, CA of SEP Bulgaria uses only the new private key for the signature of the issued certificates.

XIV. Compromising and recovery after natural disaster and accidents

SEP Bulgaria is following strict rules for the cases of compromising the private key and/or occurring of a damage, to be guaranteed recovery of the level of delivery of certification services. These procedures are conducted according to an approved plan for action at accidents and extreme circumstances.

1. Reactions to breach in security

The breaches of security of the information systems are announced immediately after their discovery to the leader of the unit who is responsible for their elimination.

The personnel of Sep Bulgaria have rights and obligations to make proposals and to make reports for breaches of security.

Defects in the software are reported directly to the operational manager or to the administrator.

The measures and procedures for action at occurring of technical problems relate to the security are described below in this section.

2. Damages on computer resources, software or/and data

The policy for security, applied by Sep Bulgaria defines the following major treats regarding the process of non-interruption of offering the services:

- Physical destruction of the systems of SEP Bulgaria including network resources – this treat includes destruction of any character mostly accidental;
- Failure in the work of the software and the applications, lack/impossibility for access to the data – these failures ate caused by the improper functioning of the operational systems and user`s applications as a result of harmful codes;
- Loss of important network services – loss of power supply and physical interruption of cables;
- Failure in the used hardware.

In order to prevent and restrict the influence of the above stated treats, SEP Bulgaria uses the following practices and security policies:

2.1. Plan for recovery after damage or natural disaster

All the users of certification services are informed in a proper way for the current situation and all the restrains at offering the services related to the functioning of the information systems and the network infrastructure. The plan includes all lot of actions depending on which part of the system is invalid or functioning with problems:

- Mirror copies of the discs are made to all servers and working stations. Each reserve copy is preserved on two places- in SEP Bulgaria and reserve center for processing of data;
- Periodically are made reserve copies of the data base. The copies contain all submitted demands, the issued, renewed and suspended certificates. The copies are preserved at the above stated places;
- Periodically is made full reserve copy of each server. This copy contains all the submitted demand, the book of events, the issued, renewed and suspended certificates. The copy is preserved at secure place outside of the office of SEP Bulgaria;
- The keys of Sep Bulgaria divided into parts are held by persons on trustful position and are preserved by them;
- A reserve equipment is situated for the change of broken servers, discs equipment for communication;
- The procedures are tested regarding to each.

2.2. Management of the changes

The installation and renewal of the software to newer versions of the operative systems is accomplished only after test installations and the test system renewed.Each modification of the system is accomplished after approval by the Security Administrator. Preliminary measures are being taken for the recovery of the system to their state before the installation or the renewal in case of problems at functioning.

2.3. Reserve systems

In case of failure or disaster SEP Bulgaria activates in the terms of 24 hours reserve systems which will replace the major functions of CSP until the basic systems will be replaced. Because of the presence of reserve copies of the systems and reserve hardware SEP Bulgaria:

- Activates the reserve center in order to provide certification cervices;
- Processes the collected and unprocessed demands for suspension;
- Processes other demands by the users of certification services.

2.4. Creation of back-up copies

SEP Bulgaria creates back-ups of all data so that it is possible to restore the system to any point of time. Copies are made also of all the data which is crucial in terms of information security of SEP Bulgaria. The copies are made periodically and kept outside the office of SEP Bulgaria. The copies are protected with passwords and encrypted.

3. Additional activities

In order to prevent cessation of operation of CSP due to power failure, backup power supply is provided. Every six months the back-up power is tested.

4. Compromising CA's private key

In case the private key of the CA of SEP Bulgaria is compromised or suspected to compromise, the following actions are taken:

- CA generates a new key pair and a new certificate;
- Notification to all users of certification services;
- Notification to the Communications Regulation Commission;
- Certificates signed with the compromised key shall be revoked with the relevant reason for termination;
- All certificates in the certification path of compromised certificate are revoked with the relevant reason for termination;
- New certificates to Holder s / Authors are generated;
- The new certificates are issued on behalf of SEP Bulgaria.

5. Restoring activities after recovery from disasters and accidents

After each system recovery from an accident, IT Security Manager and the System administrator perform the following activities:

- If necessary, change all passwords;
- Review and provide / withdraw access rights to system resources;
- Change all codes and PIN related to physical access to system components;
- Review and analyze the subject related to the accident. Correct and supplement the action plan, security policies and rules for physical access to premises and system components;

- Inform users of the system for restored system operations;
- Initiate termination or transfer of operations of the relevant system.

XV. Termination or transfer of CA's activity

SEP Bulgaria informs CRC and all Client s about its intention to terminate the activities within the statutory deadlines, specifying whether the activity will be transferred to another provider of certification services.

Upon transfer of activities to another CSP, SEP Bulgaria forward all documentation relating to its activities to the provider to whom he has transferred the business. The certification service provider who has taken management of the certificates of SEP Bulgaria is obliged to maintain them until the expiry of their validity in the terms of their issue, without further payment by the Client.

SEP Bulgaria could transfer his activities only to an accredited certification service provider and should submit all documentation relating to the operation.

SEP Bulgaria shall inform the Communications Regulation Commission in the event of the commencement of the bankruptcy, liquidation proceedings or proceedings for termination of CSP.

In case SEP Bulgaria fail to transfer its business to another accredited provider, SEP Bulgaria shall revoke the certificates and submit documents to the Communications Regulation Commission, immediately after the termination of its activities. The Communications Regulation Commission maintains a Register of revoked certificates of the CSP, after the termination of its activities.

XVI. Termination or transfer of RA's activity

Registration Authority of SEP Bulgaria may suspend its activities:

- Upon expiry of the contract governing the relationship between SEP Bulgaria and the person operating as RA;
- Upon RA each of contract and / or failure to comply with this User Guide;
- In the cases stipulated in the contract governing the relationship between SEP Bulgaria and the person operating as RA.

XVII. Technical and technological security

This section describes the procedure for generating and management of cryptographic key pairs of CA, RA and Holder / Author the technical controls accompanying the generation.

1. Generating and installing key pairs

Key management is done in a secure environment through the use of specialized cryptographic hardware and implemented by the holder of the keys.

SEP Bulgaria possesses all the keys and certificates of the CA operating in an information system:

- Root Certification Authority of SEP Bulgaria - SEP Root CA;
- Operational Certification Authority - eSign QES CA.

The private key of SEP Root CA is used exclusively for signing public keys of: eSign QES CA; SEP TSA and for signing the issued CRL.

The key pair of the Operational Certification Authority is used exclusively for signing the certificates issued to end customers, eSign OCSP and CRL.

The Operational Certification Authority signs infrastructure certificates necessary for the providing of certification services, such as:

- Signing of messages sent to the Holder / Author and RA;
- Key exchange for encrypted communication between the CA and RA.

1.1. Key pairs generation

All CA's keys are generated in protected areas of SEP Bulgaria, following approved by the CSP Management internal procedure in the presence of trusted members of the staff, notary / legal adviser and representative of the senior management of SEP Bulgaria.

Key pairs are generated using a separate workstation connected to the cryptographic module conforming to FIPS 140-2 Level 3 or to similar security requirements.

The CA's keys are generated in accordance with pre-tested and approved procedure. Records are kept of all actions performed during generation. Each record contains a description of the action, date and signature of the person who performs the action and the person supervising the execution of the action. Protocol from the procedure is signed by all present people.

RA's keys are generated by the System operator under the supervision of the IT Security Manager, by using cryptographic module conforming to FIPS 140-2 Level 2 or to similar security requirements. They are used to authenticate the request from the Holder / Author sent by RA to CA.

Holder / Author initiate the generation of key pair of their own or by RA. The Author / Holder's key pair for QES Certificate is generated only in an approved by the provider SSCD, with checked level of security and successful performance through the interfaces of the CSP's infrastructure.

1.1.1. SEP Root CA keys generation

The procedure is performed at initialization of the system for provision of certification services of SEP Bulgaria.

The procedure includes:

- Generating basic key pair;
- Installment of the private key in the cryptographic module;
- Issuance of root, self-signed certificate for CSP containing the public key and signed with the private key.

The key pair is used for signing the certificate of the operational certification authority, the "List of revoked certificates" of the Root CA and the certificate for time stamp.

1.1.2. Change of keys of SEP Root CA

The procedure for replacing the key pair is realized at the end of the validity period of the root certificate. The procedure starts at least one year before the expiry period of validity of the old key pair of SEP Bulgaria. SEP Bulgaria issues a new certificate for SEP Root CA and for one year SEP Bulgaria supports the new and the old certificate, and then the old certificate expires and new certificate of SEP Root CA remains valid.

During this year the users of certification services can use the old certificate in order to obtain a secure and reliable manner the new root certificate of SEP Bulgaria.

Since the generation of the new key pair, SEP Bulgaria disables the old private key and only the new private key is used for signing.

1.1.3. Change of keys of Operational CA

When changing the keys of the Operational CA the procedure described in Item 1.1.2 is followed and the new operational certificate is issued by SEP Root CA and signed with new private key.

1.2. Providing the private key of the Author

Upon issuance of QES Certificate the Holder / Author generate a key pair by SSCD.

If the Holder / Author expressly request the generating the key pair to the CSP, the generation is done in a secure and reliable manner, after which the CSP provides Holder / Author necessary data to access SSCD, subject to the procedure provided in "Policy in providing certification services. "

1.3. Providing the public key of CA

The Public key from key pair is provided for authentication by the CA. This is achieved by compliance with the requirements specified in PKCS # 10 Certification Request Syntax.

1.4. Providing the public key of CA to Relying parties

The public key of the CA of SEP Bulgaria is distributed as part of the electronic signature certificates issued by SEP Bulgaria. The root certificate of SEP Bulgaria is a self-signed certificate.

SEP Bulgaria distributes its root and operational certificates as follows:

- By publishing in the electronic public register of the CSP, located on the webpage of SEP Bulgaria;
- Together with user set of applications;
- The new root certificate is available for download on the website of SEP Bulgaria with measures against adulteration provisioned.

When replacement of the keys of the CA occurs, in the public electronic register the new certificates are published and records of all the old certificates are kept.

2. Key length

The length of keys used is in accordance with ORACCQES and is as follows:

Key holder	Key parameters	
	RSA	Validity
SEP Root CA	4096 bit	20 years
eSign QES CA	2048 bit	10 years

The parameters of generated keys of SEP Bulgaria are in accordance with ORACCQES.

3. Protection of private key

Private keys of CSP and its customers of certification services are generated, stored and used by devices to secure creation of the ES. Hardware cryptographic modules used by SEP Bulgaria are in accordance to Art. 26 of NDDUURNPIPUU as creating, storing and using of the private key of the CSP are carried out in a system with secured profile established in accordance with the general requirements (CC), security level EAL 4 or higher according to ISO 15408 or other specification determining equivalent levels of security.

SEP Bulgaria issues Certificates and certifies provided by the Holder / Author public keys if the key pair is generated by a SSCD with security level EAL 3 or higher.

3.1. Access to the private key of the Provider

The access to the private keys of CSP used for signing QES Certificates is performed jointly by at least two employees at trusted job positions in physically secured environment.

3.2. Back-up copies of the private key

SEP Bulgaria makes copies of its private key aiming to recover after an accident or breakdown in the systems.

The private keys of CSP used for signing QES certificates, are archived, stored and recovered jointly by at least two employees at trusted job positions in physically secured environment.

3.3. Archiving of private key

SEP Bulgaria does not keep records of private keys at the end of their life cycle. All private keys at the end of their life cycle are destroyed in such a way as to prevent their use.

3.4. Transfer of private key from and to crypto module

Transfer of the private key of SEP Bulgaria from crypto device could be needed when making a backup copy of the key.

Transfer of the private key of SEP Bulgaria to crypto device could be needed for recovery after an accident or migration to another crypto device.

Upon transfer the private key is divided into parts and each part is encrypted with a key. Access to this key is a password known only to the holder of the secret part.

3.5. Storing the private key in crypto device

SEP Bulgaria stores its private keys in crypto devices, access to which is made at least by two duly authorized employees at trusted job positions.

3.6. Activation of private key

The private key of SEP Bulgaria is activated after transferring all separate secret parts in the crypto device and PIN code for activation is entered by each holder of a single part. Activation is carried out at least by two duly authorized employees at trusted job positions.

3.7. Deactivation of private key

The private key of SEP Bulgaria is disabled by starting a procedure for initialization of crypto device. Disabling is carried out at least by two duly authorized employees at trusted job positions.

3.8. Destruction of private key

The private key of SEP Bulgaria in crypto device is destroyed by starting a procedure for initialization of crypto device. Destruction is carried out at least by two duly authorized employees at trusted job positions.

A procedure is followed for destruction of all separate parts of the private key of the CSP.

3.9. Crypto device certification

Used crypto devices of SEP Bulgaria in providing certification services meet the requirements of EDESA and regulations for its implementation. SEP Bulgaria provides certificates for cryptographic security of the used crypto devices.

XVIII. Other aspects of key management

1. Archiving of public key

The public keys of SEP Bulgaria are stored as part of QES Certificate and are archived 10 (ten) years after the expiration of their validity. Until archiving, the Certificates of SEP Bulgaria's CA are available through the public electronic register.

2. Validity period of Certificates and key usage

The maximum validity period of certificates used by SEP Bulgaria in the provision of certification services and the maximum period of use of the relevant private key is as follows:

Certificate	Period	
	Certificate validity	Private key usage
SEP Root CA	20 years	19 years
eSign QES CA	10 years	9 years
SEP TSA	10 years	10 years
eSign OCSP	10 years	10 years
eSign Qualified Private	3 years	3 years
eSign Qualified Organization	3 years	3 years
eSign Qualified Profession	3 years	3 years

3. Activation data

The data for the activation of key pairs, PIN and / or passwords and codes of SEP Bulgaria is divided into secure parts and are held by various employees of trusted job positions. SEP Bulgaria follows a special procedure for collection and

use of activation data, which ensures protection against unlawful and unauthorized use of key pairs. Each separate part is protected by a separate code and / or password or code.

Activation data is generated in a secure and safe way during the process of generating separate parts.

Data for activating the access to the private key of customers of the CSP is generated during the procedure for issuing the QES Certificate when the issuance is related with provision of SSCD to the Customer.

Access data for Customer's crypto device (PIN / PUK codes) are provided to Customer in a sealed envelope or in another safe and reliable manner, providing their inability to compromise.

It is permitted that access data to Customer's crypto device is provided to the Author by the Holder or his representative when it is requested in the request form.

Holder / Author must change the access data to the provided Customer's crypto device (SSCD) as soon as they get it.

XIX. Computer security management

1. Technical requirements

The described technical requirements rely to computer systems and installed system software used for system operations. The computer system protection is implemented at the following levels - operating system, application software and physical access.

The computer systems located in CA, implement the following controls:

- Required authentication of operating system and system applications;
- Keeping a log with operators' activities;
- Access to systems is allowed only to duly authorized employees of SEP Bulgaria;
- The exchange and databases are protected by encryption.

1.1. Security assessment

SEP Bulgaria assesses the security of the computer systems and technologies used for providing certification services periodically.

1.2. Technical controls

2. Information security controls management

The aim of the management of information security controls is to ensure that the systems of SEP Bulgaria function properly in accordance with their settings and configuration.

Any changes to system settings and configurations are tested, monitored and recorded.

2.1. Network security

SEP Bulgaria's servers and trusted workstations are connected in separate internal local network. Access to the Internet is controlled by the firewall and break-in detection sensor.

SEP Bulgaria takes measures to ensure flawless operation of the systems for providing certification services and ensure reliability and security of data exchange between RA and CA. Additional measures are taken in monitoring and reporting of breaking-in attempts and blocking operations connected to certification services providing.

XX. Certificates' Profiles, CRL and OCSP

All profiles of certificates for electronic signatures and CRL are defined in accordance with RFC 3280 and ITU-T X.509 v.3. The OCSP profile is in accordance with RFC 2560, and Time stamp profile is in accordance with RFC 3161.

1. Certificates profiles

Fields included in the certificates' content and their interpretation form the profiles of certificates issued in the entire hierarchy of SEP Bulgaria.

2. Certificate content

SEP Bulgaria maintains a set of fields and attributes in issued QES certificates. The presence or absence of certain attributes in the fields depends on the type of the issued QES certificate.

SEP Bulgaria defines a set of extensions for the certificates. Some extensions are marked as critical to ensure proper use of certificates. Applications that use certificates must reject any certificate that contains a critical extension that is unrecognized. Below is a general description of supported fields and extensions of SEP Bulgaria.

- Version: third version (X.509 v.3);
- SerialNumber: Unique serial number of the certificate in the issuing Certification Authority;
- Signature: identifier of algorithm used from issuing certification authority for signing the Certificate;
- Issuer: Distinguished Name of issuing certification authority;
- Validity: Certificate validity period. Start date (notBefore) and end date (notAfter) are described for validity period;
- Subject: Distinguished Name of Holder / Author;
- SubjectPublicKeyInfo: the value of public key together with the identifier of the associated to it algorithm;
- SignatureAlgorithm: identifier of algorithm used from issuing certification authority for signing the Certificate;
- SignatureValue: Certificate's electronic signature (calculated based on all fields of the main field: version, serialNumber, signature, issuer, validity, subject, subjectPublicKeyInfo; signatureAlgorithm is used).

Possible values of individual fields are listed in the table below:

Name of Field	Value or limitation of value	
version	Version 3	
serialNumber	Unique serial number of the certificate in the issuing Certification Authority	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
issuer	countryName	BG

Name of Field	Value or limitation of value	
(Distinguished Name)	localityName	Sofia
	organizationName	System for Electronic Payments/SEP Bulgaria JSC
	organizationalUnitName	SEP
	commonName	eSign QES CA
	Street	1 Zlatovrah Str.
validity	notBefore	UTCTime format
	notAfter	UTCTime format
subject (Distinguished Name)	Distinguished Name of Holder / Author compliant with the requirements of X.501. The values of attributes depend on the type of issued certificate.	
	*C, Country	Defines the context in which other attributes are considered.
	ST, State or Province	If used, contain geographic information related to Holder. If organizationName is present, that information is related to the organization.
	*L, Location	
	O, Organization	If used, contain the name of the organization, which is associated with the Holder and the related organization information.
	OU, Organization Unit	Contain the type of certificate issued.
	UID, Unique Identifier	EGN/UCN of Holder
	*CN, Common Name	Author's name / alias
	T, Title	If used, contain Author's job position or function in Holder's organization.
	Street	Address – str, No, bl., apt. of the Author
	PostalCode	Holder 's postal code
	Phone	Holder 's phone number
	*EmailAddress	Author's email for correspondence related to Holder.
Key Usage	{digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyCertSign, cRLSign}	

Name of Field	Value or limitation of value
Enhanced Key Usage	{serverAuth, Client Auth, codeSigning, emailProtection, timeStamping, OCSPSigning}
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=eSign QES CA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eSign.bg [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/
CRL Distribution Points	1]CRL Distribution Point Distribution Point Name: Full Name URL=http://crl.sep.bg/SEP_root_ca.crl

Name of Field	Value or limitation of value
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	cA: yes/no, Path Length Constraint=None
Subject Alternative Name	Author's address
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	Author's public key and the algorithm to be used
Qualified Certificate Statements	Defines the certificate as certificate issued for qualified electronic signature
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
signatureValue	CSP electronic signature

Standard extensions

SEP Bulgaria supports the following extensions:

- Authority Key Identifier: identifies the CA's public key corresponding to the private key used for signing of the issued certificate. This extension is not critical;
- Subject Key Identifier: identifies certificate with specific public key. This field is not critical;
- Key Usage: defines the purposes for which the key from the certificate could be used. This imposes restrictions on the validations that could be made through the public key of the certificate. This extension allows to distinguish the use of different keys. Possible values are:
  - digitalSignature: validation of electronic signature;
  - nonRepudiation: for ensuring the fact of electronic signature application;
  - keyEncipherment: for secured key exchange;
  - dataEncipherment: for data encryption;
  - keyCertSign: for electronic signature of certificate validation;
  - cRLSign: for electronic signature of CRL validation;

The extension Key Usage is critical.

- Enhanced Key Usage: defines applications which can be used by the key of the certificate. This extension defines one or more fields in addition to the Key Usage field for allowable usage of the certificate. These areas should be considered as a limitation on the permissible usage. There may be one or a combination of the following elements:
  - serverAuth: for TLS WWW server authentication. Compatibility with digitalSignature, keyEncipherment or keyAgreement;
  - Client Auth: for TLS WWW Client authentication. Compatibility with digitalSignature and/or keyAgreement;
  - codeSigning: for signing of executable code mostly distributed through Internet. Compatibility with digitalSignature;
  - emailProtection: for e-mail protection. Compatibility with digitalSignature, nonRepudiation, and/or (keyEncipherment or keyAgreement);
  - timeStamping: attaches hash of object to specific time. Compatibility with digitalSignature and/or nonRepudiation;
  - OCSPSigning: signing of OCSP response. Compatibility with digitalSignature and/or nonRepudiation;

  This extension is not critical.

In the presence of two extensions Key Usage and Enhanced Key Usage, then both extensions are processed by the application separately and the Certificate is used for purposes that are compatible with both extensions. Otherwise it is not used for any purpose.

- Certificate Policies: identify one or more policies through OID policy identifier and additional policy qualifiers;
- CPSuri: index / reference in the form of a URL, to the place where the "Practice for providing of certification services" could be found;
- UserNotice: reference to the text that appears on relying parties during QES validation. The text can be inferred by reference noticeRef or to be part of the certificate explicitText.

The extension is not critical.

- Policy Mappings: Uncritical extension containing one or more pairs of OID, which define the equivalence of policies;
- Issuer Alternative Names: alternative name of the issuer of the certificate. The field is not critical;
- Subject Alternative Name: alternative name of Holder /Author of the certificate. The field is not critical;
- Basic Constraints: identifies CA (shows that public key belongs to CA) and the number of CAs in the hierarchy till the user's certificate. It may be critical for the CA and not critical in other cases. It is used with keyCertSign;
- CRL Distribution Points: shows how and where to get CRL. There may be more than one mechanism for extracting the CRL, for example LDAP or by HTTP. The field is not critical;
- Authority Information Access: defines access to information or services provided by the issuer of the certificate. Most often for online validation of certificates. The field is not critical;
- Qualified Certificate Statements: shows that the certificate is issued as certificate for qualified electronic signature.

XXI. Monitoring and control of activities

1. Frequency and circumstances for monitoring and control

Control over the activities of SEP Bulgaria acting as CSP under EDESA is performed by the Communication Regulation Commission and the Executive Agency "Bulgarian Accreditation Service".

SEP Bulgaria performs constant internal control, executed by internal auditors.

For the purposes of the internal control are conducted periodically complete or partial audits of separate activities and / or units of the infrastructure for providing certification services.

SEP Bulgaria exercises constant control over the registration authorities activities.

2. Identification and qualification of controllers

Persons in charge of audits and control are specifically authorized by the Communications Regulation Commission, the Executive Agency "Bulgarian Accreditation Service" or by SEP Bulgaria.

For performing an audit external organizations and / or persons who are accredited to carry out such audits could be attracted.

Audits of the operation of registration authorities are carried out by employees of the CSP expressly authorized by SEP Bulgaria or external audit organization.

3. Avoiding conflict of interest

The relationship between external controllers in cases other than those performed by the state authorities and SEP Bulgaria, is covered by a written contract.

4. Scope and detail of audits

The scope and detail of the performed audits depends on the kind of the audit and inspected units.

In the scope of internal audit are all activities, documents and circumstances of the operation of CSP, which may include, but are not limited to:

- Compliance of procedures and practices of SEP Bulgaria with the defined in the User Guide procedures and policies;
- Strictly following of procedures and practices specified in the User Guide from employees and departments responsible for providing certification services;
- Adherence to procedures and practices specified in the User Guide from the external Registration Authorities;
- Management of the infrastructure for providing certification services.

5. Measures for avoiding deficiencies

The inspection report is considered by management board of SEP Bulgaria. All gaps are analyzed and measures are taken to to remedy them.

6. Results communication

The audit results are made available to the inspected units. Records for inspections are kept. The results of the audits are kept following the terms and conditions specified in the User Guide.

XXII. Commercial and legal terms

1. Tariff for providing certification cervices

SEP Bulgaria as a CSP determines the prices of provided certification services. Pricing information for certification cervices and related to their providing administrative services are published in the "Tariff of SEP Bulgaria for providing certification services" (Tariff) on the webpage of SEP Bulgaria.

SEP Bulgaria reserves the right at any time to change the tariffs for the services. Tariff changes take effect within 7 (seven) days of their publication on the website of SEP Bulgaria. Price changes are effective and binding for all Client s of SEP Bulgaria, who at the time of entry into force of the changes are using the services of SEP Bulgaria and have not claimed within the specified period in the contract disagreement with these changes.

1.1. Due amounts under the contract

Fees payable by Client s under the signed contracts are formed, based on the certification services they use under the contract and in accordance with the current Tariff at the time of maturity of the obligation.

In case of delay by the Client to pay the amounts due, he shall pay a penalty in the amount of statutory interest for delay.

Paid amounts by the Client are not subject to refund upon termination of his relationships with CSP, regardless of the reason.

1.2. Payment and invoicing

CSP issue an invoice to the Client for the paid fees for certification services within the statutory deadlines. Failure to pay on time or partail payment of amount due from the Client is a reason to CSP to terminate the provision of customer services.

All sums due are paid in cash at Registration authorities or in a bank. Payments by bank transfer are deemed to be effected at the time of crediting the bank account of SEP Bulgaria with the full amount due.

All bank taxes and commissions regarding payment by bank transfer are covered by the Client.

2. Financial responsibility

2.1. Insurance of activities

SEP Bulgaria insures its activities acting as CSP under EDESA and other regulations related.

The subject of insurance is the responsibility of SEP Bulgaria as a provider of certification services for caused material and immaterial damages to the Author / Holder and all third party following meeting the requirements of Art. 29 of the EDESA and other reference legislation.

SEP Bulgaria has a contract for insurance for minimal amount of 600 000 leva for each affected person from each event.

When such event occurs, the affected person is required within 7 (seven) days to place written notice to SEP Bulgaria and the insurer of SEP Bulgaria.

2.2. Insurance coverage for Users

SEP Bulgaria compensates by insurance every affected person in any event within the limit set by the limitation of the application of the issued certificate.

For the avoidance of doubt, insurance does not cover and CSP is not responsible for cases of damage resulting from:

- Failure to comply with obligations under the "Practice in providing of certification services";
- Compromise or loss of private key of the Holder , Author respectively, because of improper care for the protection or its use;
- Non-compliance with the requirements on diligence for verification by Relying Parties to the validity of electronic signatures and certificates issued by the CSP;
- Force majeure, accidents and other events beyond the control of the CSP.

3. Information confidentiality

SEP Bulgaria complies with all applicable rules for the protection of personal data and sensitive information collected with regard to his activities as a provider of certification services, following the procedures as described in the User Guide.

3.1. Scope of information confidentiality

SEP Bulgaria accepts as confidential the information contained in or relating to:

- Holder / Author, except published in the certificate;
- Agreement for certification services;
- The reason for suspension or revocation of certificates for QES beyond the published information on the status of the certificate;
- Correspondence relating to the acting of SEP Bulgaria, as a provider of certification services;
- Private keys of SEP Bulgaria;
- Records of requests made for the issuance, suspension, reactivation and revocation of certificates;
- Records of transactions;
- Records of external and internal audits and reports;
- Plans for disaster recovery and contingency.

3.2. Information beyond the scope of information confidentiality

SEP Bulgaria does not consider as confidential the information contained in or relating to:

- The Certificates published in the Register of CSP;
- The data contained in the certificates;
- The data on the status of certificates published in the "List of revoked certificates";
- Any other information that is publicly available and / or known.

3.3. Obligations for keeping confidential information

SEP Bulgaria does not reveal and could not be asked to disclose or provide to third parties any confidential information unless special law requires disclosure of such information to the competent authority.

Registration Authorities, Holder / Author or their authorized persons if the Holder is a legal entity should not disclose or allow distribution of information made known to them during or in connection with their obligations under contracts with SEP Bulgaria without prior written permission of SEP Bulgaria.

4. Protection of personal data

CSP collects data and information of the Holder / Author for the purpose of issuing and maintaining certificates for electronic signature.

CSP collects, processes, stores and provides access to such personal data to third parties in compliance with the Law on Personal Data Protection.

CSP is registered as an administrator of personal data by the Commission for Personal Data Protection under the Law on protection of personal data.

CSP shall inform aforetime persons about the types of information collected about them.

5. Intellectual property rights

SEP Bulgaria owns and retains all intellectual property rights over databases, websites, trademarks and logos used by SEP Bulgaria (e.g. eSign), electronic signature certificates issued by SEP Bulgaria and any other documents developed and supported.

SEP Bulgaria permit issued certificates without restriction by the Author to be copied and distributed provided they are reproduced as a whole.

All rights on RA ands, trademarks and logos are retained by the holder s of these rights. SEP Bulgaria uses the objects of such rights only for the purpose of providing certification services.

The key pairs and secret parts of the private keys of SEP Bulgaria are the property of SEP Bulgaria.

6. Duties and responsibilities

6.1. Duties and responsibilities of SEP Bulgaria

SEP Bulgaria is accredited provider of certification services according to § 41 of the Law amending the Electronic Document and Electronic Signature Act, promulgated in State Gazette No. 100 of 2010 and operates in accordance with the reference legislation. In this respect SEP Bulgaria shall ensure that:

- Comply with all provisions of EDESA and regulations for its implementation;
- Follow strictly defined procedures and policies regarding issuing and management of certificates for qualified electronic signature, as reported to the Communications Regulation Commission;
- The information included in the issued certificate is accurate and complete and matches the information provided at the time of data validation.

SEP Bulgaria is responsible to the Author, respectively, to the Holder of QES and all third parties for damages:

- From unfulfillment of the requirements of art. 21 EDESA and its obligations under Art. 22 and 25 of EDESA;
- From incorrect or missing data in the certificate at the time of issuance;
- Caused in the event that during the issuance of the certificate the person named as an Author is not holding the private key corresponding to the public key;
- From algorithmic gap between private key and public key written in the certificate.

6.2. Duties and responsibilities of Registration authorities

RA act on behalf of SEP Bulgaria. People/entities start activities as RA of SEP Bulgaria after training and authorization. SEP Bulgaria controls and audits the activities of its RA on a regular basis. The relationship between the person/entity operating as RA of SEP Bulgaria and SEP Bulgaria is governed by contract.

SEP Bulgaria ensures that:

- RA comply with all provisions of EDESA and regulations for its implementation;

- RA follow strictly defined procedures and policies for issuing and management of certificates for qualified electronic signature, as reported to the Communications Regulation Commission;
- RA perform identification and authentication of all persons who request issue of a Certificate of QES;
- RA sign contracts with Client s and accept all type of requests for certification services in accordance with the provisions of this Guide;
- The information confirmed by RA operator and included in the issued Certificate is considered accurate and complete and and matches the information provided at the time of data validation.

6.3. Duties and responsibilities of Author / Holder

The Holder signs Contract for certification services with SEP Bulgaria in person or through duly authorized person.

The Holder guarantees:

- For actions of Authors, for which the Holder has requested a QES certificate;
- That the Author is authorized to make electronic statements on his behalf and hold the private key corresponding to the public key in the Certificate;
- That he has submitted accurate, complete and accurate information to the CSP in accordance with the requirements of this Guide;
- That the key pair will be used only for the relevant QES and in accordance with any limitation provided in legislation and in this Guide;
- To exercise due care to prevent any unauthorized use of the private key of the Author;
- That if the Holder / Author generate the key pair alone:
  - o use only algorithms approved as suitable for the purpose of QES;
  - o use the key length, approved as suitable for the purpose of QES.
- The private key of the Author is used only under the supervision of the Author;
- That he will notify the CSP immediately if any of the following events occur before the end of the validity period specified in the Certificate:
  - o Loss of the private key of the Author, theft, suspected compromise;
  - o Lost control over the private key of the Author due to compromise of activation data (eg PIN) or otherwise;
  - o Incorrect, incomplete or altered content of Certificate.
- In the event that he is informed that the CSP issuing Author's Certificate has been compromised, to ensure that the Certificate will not be used by the Author any more.

The Author is responsible to third parties as if:

- Does not perform exactly the security requirements set by the CSP;
- Does not request the CSP revocation of a certificate in cases when the private key has been used improperly or there is danger of unauthorized usage.

The author is responsible to third parties as to false statements made to the CSP and related to the content or the issuing of the Certificate.

When the certificate is issued with registered Holder, the Holder is responsible for the failure by the Author of the obligations under the preceding paragraphs.

6.4. Duties and responsibilities of Author / Holder to the CSP

The Author / Holder are responsible to the CSP, if the Author has provided false information respectively kept information related to the content or the issuance of the certificate, and in case he is not holding the private key corresponding to the public key of the Certificate.

6.5. Duties and responsibilities of Relying Party

The Relying Party is responsible for checking the validity of the QES certificate in accordance with Section VII, p.7.2 of this Guide and for the use of QES certificates in accordance with the provisions of p.25, as their actions comply with the restrictions included in the QES certificates.

7. Limitation of liability

SEP Bulgaria bears liability only for damages referred to in p. 6.1. Of this section. For the avoidance of doubt, SEP Bulgaria is not responsible for:

- Lost profits or other consequential damages arising out of or in connection with the use or inability to use the QES certificates and electronic signatures;
- Any damage other than those associated with reliance on the information specified in the QES Certificate based on confirmed information;
- Using of QES Certificate, which is not valid or specified limits are exceeded specified in the Certificate or in this Practice;
- Security, usage, integrity of products, including hardware and software that Holder / Author are using;
- Compromised private key of the Author;
- Violation of the rights of third parties regarding their trademarks, trade names or other material or immaterial rights when information contained in Certificates issued, has led to such violations;
- Damage resulting from negligence, lack of care or knowledge in relation to QES certificates usage;
- Damage resulting from untimely revocation and / or suspension of certificates and validation the status of certificates.

8. Limit of liability

SEP Bulgaria limits the effect of electronic signatures and the certificates of electronic signatures to a limited property interest. SEP Bulgaria limits his liability within the following limits:

QES Certificate type	Liability limit
eSign Qualified Private	60 000 leva
eSign Qualified Organization	60 000 leva
eSign Qualified Profession	60 000 leva

These limits of liability shall be deemed to limit the liability of CSP within the meaning of Article 29, paragraph 3 EDESA.

These limits are maximum limits within which SEP Bulgaria is responsible for damages suffered when using issued by him Certificates for qualified electronic signatures.

9. Indemnity

In any event of failure of duties by the Holder breaching the User Guide or the Agreement for certification cervices, SEP Bulgaria will claim compensations for damages suffered.

CHAPTER III

POLICY FOR PROVIDING CERTIFICATION SERVOCES

I. Scope and purpose

This chapter provides an overview of the policy of providing certification services of SEP Bulgaria as a registered certification service provider (CSP). Presents the general concept of SEP Bulgaria on providing certification services. It defines the parties involved in the process of providing certification services, their duties, and types of certificates for QES, the process of identification and authentication as well as the applicable area of certificates issued for qualified electronic signature.

Detailed description of the processes and procedures followed by SEP Bulgaria as registered certification service provider (CSP) are provided in "Practice in providing certification services" of SEP Bulgaria.

II. Overview

SEP Bulgaria as a registered certification service provider performs the following activities:

- Issues certificates for qualified electronic signature pursuant to art. 24 EDESA and keep a register of them;
- Provide each person with access to published certificates for qualified electronic signature;
- Provide services on the creation of private and public keys for qualified electronic signature;
- Provide and / or approve devices for creating an electronic signature;
- Provides time stamp services pursuant to Art. 40 EDESA, certifying the date and time of submission of signed with qualified electronic signature, electronic document.

SEP Bulgaria provides certification services by Certification Authority and Registration Authorities.

Certification Authority and Registration Authorities carry out their activities in providing certification services on behalf of SEP Bulgaria.

III. Certification Services Model

SEP Bulgaria defines the following process model for providing certification services:

1. Registration

“Registration” covers processing and record of data in the process of submitting and accepting a Request, including data verification by eligible resources, the identity of the Author and the Holder , and if necessary - other data for these individuals. Part of the registration service covers processing the applications for management - suspension, reactivation and termination of QES certificates.

2. Creating Certificates

The technology service "Creating Certificates" includes the creation, signing and publishing the certificate in the "List of issued certificates" based on data verified in technology service "Registration".

3. Suspension of Certificates

Technology service "Suspension of Certificates" includes the processing and execution of requests for suspension and / or revocation of the QES certificates.

4. Checking the status of issued certificates

The technology service "Check the status of Certificate" is the service for providing information about the status of QES Certificate to the relying parties. This is achieved by spreading the "List with Revoked Certificates" or by service providing information about the status of the QES certificate in real time. Information on the status of QES certificates regularly.

5. Provision of equipment

The technology services "Provision of equipment" means to provide customers with encryption device or other devices for secure electronic signature creation device (SSCD). The devices are prepared and made available to the authors directly or in a secure manner by the Holder. The Service, where applicable, includes the preparation, production and delivery to the Authors / Holder s of devices and all data necessary for activation and access to them.

6. Time stamp

This service provides a certificate for the time of submission of an electronic signature created for a specific document.

IV. Level of Detail

This policy sets out the general principles of the requirements for the organization of work in connection with the provision of certification services, which are implemented by the CSP.

SEP Bulgaria, where appropriate develop, implement and document internal operating instructions, instructions or rules related to the practices and policies, which detail specific tasks execution or specify the responsibilities associated with daily operations in the provision of certification services. These rules are not public.

The policy is defined independently of the specific details of the operating environment of the CSP.

V. Requirements to the CSP

SEP Bulgaria, as a registered CSP, implement controls that meet the requirements defined in this policy.

In carrying out the provision of certification services, SEP Bulgaria acts in compliance with the current policy and regulations of the Republic of Bulgaria in the field of certification services.

SEP Bulgaria has the necessary technology, hardware, software, facilities and personnel to provide certification services under EDESA and this Policy.

In accordance with this Policy, SEP Bulgaria declares in its Practice for providing Certification Services that:

- Observe EDESA and all related regulations, as well as all practices and procedures based upon the requirements specified in this Policy;
- Specify obligations to third parties relating to the provision of certification services, including the applicable policies and practices;
- Publishes and provides access to both his "Practice for providing Certification Services" for all users of certification services and also to other documents necessary to determine compliance with the certification policy;

- Determines senior management body to manage and approve practices in providing certification services under this policy and submit to the Communications Regulation Commission for approval;
- Engage senior management and its responsibility for establishing practices in providing certification services and their compliance;
- Define process for review of the practices for the provision of certification services, including the responsibility for their maintenance;
- Inform immediately of any changes in his "Practice for providing Certification Services," documents the algorithms used and their parameters.

VI. Infrastructure for the delivery of certification services - Key management

1. Generating the keys of CSP

SEP Bulgaria applies reliable process for generating its private keys. Generation takes place in a protected environment. SEP Bulgaria divides the private keys in secret parts. SEP Bulgaria is the holder of private keys, for which uses the procedure for allocating the secret parts. SEP Bulgaria is entitled to transfer such secret parts to persons who are expressly authorized.

1.1. Protected Environment

Physical access to the protected part of the systems of SEP Bulgaria is limited and it is only accessible to duly authorized employees, depending on their job descriptions.

1.2. Authorized personnel

Used practices for personnel management include measures that provide guarantees of reliability and competence of staff to fulfill their obligations.

1.3. Sharing the secret parts

SEP Bulgaria uses sharing of the secret parts of its private keys and distributes them among authorized persons whose responsibility is keeping the secret parts.

1.4. Reliable systems

SEP Bulgaria operates reliable systems in the provision of its certification services and in the generation of the key pairs. The reliable system comprises of computer hardware, software and procedures to ensure an acceptable level of protection against risks related to security, provides a reasonable level of performance, reliability, proper operation and execution of security requirements.

2. Generating the keys of SEP Bulgaria

SEP Bulgaria generates in a secure way and protects its own private keys using a reliable system and takes all the necessary measures to prevent compromise or unauthorized use.

2.1. Starting procedure

SEP Bulgaria implements and documents the starting procedure for generating the keys, in accordance with this Policy. SEP Bulgaria applies European and generally recognized in international practice standards for reliable systems and does everything possible to follow them.

2.2. Cryptographic Hardware

The generating of the keys of SEP Bulgaria is performed by hardware cryptographic device for creating, storing and using of the private key with the security level EAL 3 or higher according to ISO 15408 or other specification, determining equivalent levels of security.

2.3. Algorithms used

The keys of SEP Bulgaria are generated using algorithms that are recognized as suitable for the purpose of issuing certificates for qualified electronic signature and meet the requirements of the "Regulation on the algorithms to create and verify qualified electronic signature".

2.4. Length of key

The selected length and algorithms of keys signing issued certificates for QES are recognized as suitable for the purpose of issuing certificates for qualified electronic signature.

2.5. Ensuring continuity of operations

Before the validity expiration of the keys signing the issued certificates for QES, SEP Bulgaria generates a new key pair for signing certificates and apply all necessary measures to avoid disruption of operations of each party may rely on the keys of the CA. New keys are generated and distributed in accordance with this Policy.

3. Storage, backup and restore the keys of CSP

SEP Bulgaria provides confidentiality and integrity of its private keys.

3.1. Possession and use of private key

The private keys of CSP used for signing certificates for QES, are held and used, without leaving the secure cryptographic device that is at security level EAL 3 or higher according to ISO 15408 or other specification, determining equivalent levels of security .

3.2. Protection of private key

When private keys are outside the secure cryptographic device, they are protected in such a way that provides the same level of protection as is provided by a secure cryptographic device.

3.3. Backup of private key

The private keys of CSP used for signing certificates for QES, are archived, stored and recovered by at least two employees together at trusted job positions in physically protected environment.

3.4. Copies of the private key

During the controlled procedure for creating backups of the private keys of CSP used for signing certificates for QES, apply equal or higher security measures as those used during operation.

3.5. Storage of private keys of CSP

When the keys are kept in specialized hardware module, a mechanism for access control is implemented which ensures that the keys are inaccessible outside the hardware module.

3.6. Distribution of public keys of CSP

SEP Bulgaria takes measures to ensure maintenance of the integrity and authenticity of the public keys of CSP used to verify the electronic signature and all parameters associated with it.

3.7. Source and integrity of the public key

The public keys of CSP used to check the electronic signature are available for all participants in the certification process in such a way that ensures the integrity of public keys and the verification of their origin.

3.8. Protecting the private key of the provider

Only CSP has access to the private key. The private key is not provided in any form or by any means to other persons for use or storage.

4. Using the keys of CSP

SEP Bulgaria as CSP provides appropriate use of its private keys.

The private keys of CSP used in generating Certificates for QES can be used for signing other types of certificates as well as the information about the status of issued certificates for QES so far this usage has not violated the requirements defined in this document.

5. Physical Protection

The Private keys of CSP used for signing certificates for QES can only be used in physically protected environment.

6. Termination of the life cycle of the keys of CSP

SEP Bulgaria takes measures to ensure that the private keys of CSP used for signing certificates for QES can not be used after the end of their lifecycle.

All copies of the private keys of CSP used for signing certificates for QES and the data for their generation, shall be destroyed or put non-operational.

7. Life cycle of cryptographic hardware used for signing Certificates for QES

SEP Bulgaria takes measures to ensure protection and security of the cryptographic hardware during its life cycle.

7.1. Delivery of cryptographic hardware

The cryptographic hardware used for signing certificates for QES and the information about issued QSE Certificates has not been compromised during delivery.

7.2. Storage of cryptographic hardware

The cryptographic hardware used for signing QES certificates and the information about the status of issued certificates has not been compromised during storage.

7.3. Joint control

Installation, activation, backup and recovery of the private keys of CSP used for signing QES Certificates in the cryptographic hardware is implemented from at least two employees at trusted job positions.

7.4. Operation of the cryptographic hardware

The cryptographic hardware used for signing QES certificates and the information about the status of issued certificates functions correctly.

7.5. Destroying of private keys in cryptographic hardware

Private keys of CSP used for signing QES certificates stored in the cryptographic hardware are destroyed when the hardware is no longer used by the CSP for this purpose.

VII. Providing services in key management of the Holder / Author

In case SEP Bulgaria provides services to the Holder / Author of key management, SEP Bulgaria takes measures to ensure the secure generation of keys for the Author and the secrecy of the private key of the Author.

1. Used algorithms

In cases where the CSP generates the keys for the Author, it uses algorithms that are recognized as suitable for use for the purpose of the QES, for the period of validity of the certificate issued to it.

2. Key length

In cases where the CSP generates keys for the Author, it uses keys' length recognized as suitable for use for the purposes of the QES, for the period of validity of the certificate issued to it.

3. Generated keys storage

In cases where the CSP generates the keys for the Author, CSP provides the tools for secure creation and storage of the keys of the Author (SSCD), until their delivery to the Author in a secure manner.

4. Delivery of keys

In cases where the CSP generates the keys for the Author, private keys are delivered to the Author, so as not to compromise their security and integrity. Once delivered, private keys are under the exclusive control of the Author.

4.1. Preparation of SSCD

CSP provides a secure and reliable issuance and storage of QES Certificates by SSCD.

4.2. Control on the preparation of SSCD

The preparation of SSCD is performed in a safe and controlled manner by the CSP. The used SSCD are under the security level EAL 3 or higher according to ISO 15408.

4.3. Storage and delivery of SSCD

The storage and distribution of SSCD is performed in a safe and controlled manner by the CSP. SSCD is provided to the Author, if necessary by the Holder so as not to be compromised.

4.4. Deactivation and reactivation of SSCD

Deactivation and activation of SSCD is performed in a safe and controlled manner by the CSP.

5. Data for activation

Where to SSCD is associated user activation data (PIN), this data is prepared safely and distributed separately from the SSCD. Separation may be time, place, or both.

If the activation data is not separated from SSCD, it shall take additional measures to prevent its compromise with the appropriate security measures.

VIII. Infrastructure for providing certification services - QES Certificate Lifecycle Management

1. Registration of Holder / Author

SEP Bulgaria takes measures to ensure proper identification and authentication of applicants for QES Certificates , check their empowerment, and acceptance of complete and accurate requests for issuance of QES Certificates.

1.1. Providing information for certification services

Before signing a contract for certification services with the Holder, the CSP informs the Client s, respectively, his representative, about the terms and conditions on certificates' usage. Detailed information is presented on SEP Bulgaria website.

1.2. Checks during registration

During registration the CSP within the meaning of Section III, p.1. verifies by acceptable means, in accordance with national law the identity, if applicable, other information about the person to whom the QES Certificate is issued. Verification of proofs of identity of the individual, can be done both directly and indirectly, in which case means of providing equivalent to physical presence security are used.

2. Identification of individuals

Individuals must provide evidence of:

- The full name of the individual - Author and Holder;

- National identity number or other data that can be used to distinguish the person from others with the same name.

3. Identification of legal entities

Where for the purpose of issuing the QES Certificate, an individual associated with the entity or organization is identified, he must provide evidence of:

- The full name of the individual - Author;
- National identity number or other data that can be used to distinguish the person from others with the same name;
- Full name and legal status of the associated legal entity or organization - Holder;
- Any relevant registration information or information from a register;
- Evidence that the individual - Author represents the legal entity, organization or individual - Holder.

4. Stored information

CSP records all information used for identity verification and, if applicable, other specific attributes, including names and reference numbers of documents used in the registration and the limitations of their validity.

4.1. Representation data

If the request for a QES Certificate is placed by a person other than the Author / Holder, evidence should be provided that the applicant has been authorized to act on behalf of the Author / Holder.

4.2. Contact data

The Author / Holder shall provide contact data.

5. Contractual relations

CSP stores in its files a signed contract with the Client, which governs the rights, obligations and responsibilities of the parties.

6. Storage time

The records identified above shall be retained for a period of time for which the Client is informed and, where appropriate, for the purpose of providing evidence at trial in accordance with applicable law.

7. Possession of Private Key

If CSP has not generated the private key of the author, the process of requesting the issuance of the certificate shall ensure that the Author keeps the private key corresponding to the public key provided for certification.

8. Possession of SSCD

If CSP has not generated the key pair and certification policy requires the use of SSCD, the process of requesting the issuance of a Certificate shall ensure that the public key provided for certification, is generated by a SSCD.

9. Renewal, replacement of keys and update

CSP shall ensure that request applications for renewal, modification and management of QES certificate are complete and accurate and come from the Holder or duly authorized person. This includes changing the keys after termination or

during validity period of QES certificate when registered records should be updated following a change in the original data provided by the Author / Holder.

9.1. Current QES Certificate

In case of renewal of QES certificate, CSP shall verify the existence and validity of the QES certificate, as well as the validity of information used during the identification of the Author / Holder.

9.2. Change of conditions of SEP Bulgaria

Should the conditions for providing certification services change, CSP should inform Author / Holder on changes in the manner provided in this Guide. If any of the terms and conditions of the CSP is changed, they are communicated to the Holder who accepts them in accordance with this Guide.

9.3. Edited content of QES certificate

If a change occurs of data contained in QES Certificate, the Author / Holder shall submit information required for alteration of data provided during registration in the manner provided in this Guide. If any of the names or data on the certificate are changed or the previous certificate has been terminated, the registration information is verified, recorded and the Holder adopts them in accordance with this Guide.

10. Creating a certificate

SEP Bulgaria takes measures to ensure secure and reliable generation of certificates for qualified electronic signature.

IX. Identification

SEP Bulgaria include identifiers of certification policies to ensure the relying parties easy access to information on the terms and conditions consistent with the certification policy in accordance with which the QES Certificates are issued.

Compliance with the identified certification policy is described by the inclusion of the relevant identifiers in issued QES Certificates.

1. Policy ID

The identifier of the certification policy is:

itu-t(0)identified-organization(4)etsi(0)qualified-certificate-policies(1456)policy-identifiers(1)qcp-public-with-sscd(1)

The identifiers of the policy according to which different types of QES Certificates are issued, will be included in the content of any certificate issued in accordance with this policy for each specific type of QES Certificate.

2. Users community and QES Certificates application

QES certificates issued in accordance with this Policy shall have the meaning of qualified electronic signature as per EDESA.

The electronic signature for which the QES Certificate is issued meeting the requirements of this Policy shall have the meaning of a handwritten signature to all, including state and local government.

3. Compliance with the Policy

3.1. General information

CSP uses the identifier as defined in above, to demonstrate compliance with this certification policy.

3.2. Compliance with the Policy

Compliance with this policy by CSP means that:

- CSP complies with all obligations which are defined in this Guide;
- CSP has implemented controls which meet all requirements defined in Section V "Requirements for activity of the CSP."

X. QES Certificates Profile

Certificates issued under this certification policy include:

- Note that the certificate is issued as a certificate of a qualified electronic signature;
- Identification of the CSP and the State in which it operates;
- The names of the signatory or, if applicable, an alias that can be identified as such;
- Provision of specific attributes of the signatory to be included in the certificate, if applicable, depending on the purpose for which the certificate is intended;
- Data for verification of signature that corresponds to the data for creation a signature under the control of the signatory;
- An indication of the beginning and end of the period of certificate validity;
- Identification code of the certificate;
- Advanced electronic signature of the CSP issuing the certificate;
- If applicable limitation on the scope of the certificate;
- If applicable limitation of the amount of transactions for which the certificate can be used.

XI. Measures against forgery of QES Certificates

CSP take measures against forgery of certificates and where CSP generates the data to create a signature, guarantee confidentiality during the process of generating such data.

XII. Secure generation

If the CSP generates keys of the Author:

- The procedure for issuing a certificate is executed simultaneously with the procedure for generating a key pair by CSP;
- Private key (or SSCD) is delivered to the Author in a secure way.

XIII. Confidentiality and integrity of registration data

Confidentiality and integrity of registration data are secured and in cases when exchanged with the Holder, Author, or between different components of the infrastructure of CSP.

XIV. Check the source of registration data

When using external providers of registration services, CSP verify that registration data is exchanged with a known provider of registration services, whose identity is authenticated.

XV. Distribution of terms and conditions

CSP provides the terms and conditions of its activities to all participants in the certification process.

XVI. Published Data

CSP provides to users the terms and conditions of its activities and procedures for the usage of certificates, including:

- The application of certification policy for issuing certificates for qualified electronic signature using SSCD;
- Restrictions on usage;
- Obligations of the Client , including the requirements of policy for the use of SSCD;
- Information on how to check the status of QES certificate, including checks in the "List of revoked certificates" so that relying parties to have "reasonable reliance" on certificates;
- The limitations of liability, including the purpose / usage for which CSP accepts (or excludes) liability;
- Period of time during which registration information is stored;
- Period of time during which the CSP keeps events logs record;
- The procedures for complaints and disputes;
- Applicable legislation;
- Information on the registration of CSP by the Communications Regulation Commission or other certifications of compliance with this Policy by reference and according to which scheme.

XVII. Availability and distribution of information

The information referred to above, is available without restriction and can be distributed electronically.

1. Access upon generating

After generating, the QES Certificate is available for review and use by the Author / Holder.

2. Access limitation

QES Certificate is publicly available for review only after the explicit indication of the Author / Holder.

3. Information for Relying Party

CSP provides the Relying Party the terms and conditions for usage of certificates.

4. Providing information about QES

The information specified above is available 24 hours a day 7 days a week. In case of breakdown of the system, service or other factors outside the control of the CSP, CSP will use its best efforts to ensure the cessation of these information services for a period not exceeding the maximum period specified in the "Practice in providing certification services."

5. Availability and accessibility of information for QES Certificates

The information referred to in Section XVII is public and accessible to all.

XVIII. Revocation, suspension and reactivation of QES Certificate

CSP revokes QES certificates promptly after receipt of authorized and validated Requests for revocation of the Certificates.

1. Documentation of the procedure

CSP documents as part of its Practice, procedures for termination / suspension of QES Certificates, including:

- Who can submit information and request for revocation / suspension;
- How to submit information and requests for revocation / suspension;
- Requirements for additional information and confirmation of the request for termination;
- Whether and for what reason the certificate may be suspended;
- The mechanisms used to distribute information about terminated certificates;

2. Receipt of Requests for revocation / suspension

Requests for termination are processed immediately upon receipt.

3. Validation of requests

Requests for termination shall be validated and authenticated that are placed by an authorized source.

4. Suspension of QES Certificate before revocation

Upon receipt of the request for suspension, CPEQES certificate is suspended from the CSP till a request for termination is received or until the maximum period for suspension of QES Certificate.

5. Information on status change

The Author / Holder shall be informed of any change in the status of QES certificate.

6. Irreversibility of revocation

After revocation of the QES Certificate, its status changes to "invalid" and cannot be changed any more.

XIX. List of revoked certificates (CRL)

Updating the lists of the issued and revoked certificates for qualified electronic signature shall be performed at least every 3 (three) hours:

- Each CRL indicates the maximum time for publishing of the next CRL;
- A new CRL may be published before the time for the next publishing of the CRL;
- CRL is signed by the CSP.

1. Accessibility to the list of terminated certificates

Services for management the status of terminated Certificates are available 24 hours a day, 7 days a week. In case of breakdown of the system or due to other factors outside the control of the CSP, CSP will use its best efforts to ensure the cessation of these information services for a period not exceeding the maximum period referred to in the Practice.

2. Certificates Status

Information on the Certificates status is available 24 hours a day, 7 days a week. In case of breakdown of the system or due to other factors outside the control of the CSP, CSP will use its best efforts to ensure the cessation of these information services for a period not exceeding the maximum period referred to in the Practice.

XX. Integrity and authenticity of information about the status of QES Certificate

CSP has taken measures to protect the integrity and authenticity of the information about the status of certificates.

1. Publishing of information regarding the status of a QES Certificate

Information on the status of certificates is public and accessible to all.

2. Period of storage of terminated QES Certificates in CRL

Information on the status of certificates is kept at least until the expiry of the validity of the certificate issued.

XXI. Certificate Authority Root Certificate

The Root Certificate of SEP Bulgaria is at first place at CSP certificate hierarchy. The Certificate is issued by Certification Authority SEP Root CA and is self-signed. During generating this certificate a special procedure for secure and reliable key pair generation is followed. The private key is used for signing the certificate of the operational Certificate Authority and also the time stamping of a specific document signed with electronic signature.

The period of validity of the Root Certificate is 20 (twenty) years.

The key length is 4096 bits for RSA algorithm.

The Root Certificate of SEP Bulgaria has the meaning of certificate for qualified electronic signature pursuant to EDESA.

SEP Root CA Certificate Profile:

Field Name	Value or limitation of value	
version	Version 3	
serialNumber	Unique serial number of the certificate in the issuing Certification Authority	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
issuer (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments/SEP Bulgaria JSC
	OU	SEP
	CN	SEP Root CA
validity	notBefore	UTC format
	notAfter	UTC format

Field Name	Value or limitation of value	
subject (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP
	CN	SEP Root CA
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Notice Text=SEP Bulgaria JSC – accredited certification service provider [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/ [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Notice Text=SEP Root CA [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eSign.bg	

Field Name	Value or limitation of value
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/SEP_root_ca.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=CA Path Length Constraint=None
Issuer Alternative Names	
Subject Alternative Name	
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	The Author's public key and algorithm to be used
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	CSP Electronic signature

XXII. Operational CA Certificate

The Operational CA of SEP Bulgaria sign issued certificates for qualified electronic signature and include the identifier of the policy according to which certificates are issued and the identifier of the type of certificate issued. The Operational Certificate is issued by the Root CA.

The period of validity of the Operational Certificate is 10 (ten) years.

The key length is 2048 bits for RSA algorithm.

The Operational Certificate of SEP Bulgaria has the meaning of certificate for qualified electronic signature pursuant to EDESA.

The Operational CA eSign QES CA issues certificates for qualified electronic signature in accordance with Policy OID: 1.3.6.1.4.1.30299.2.1.

eSign QES CA Certificate Profile:

Field Name	Value or limitation of value	
version	Version 3	
serialNumber	Unique serial number of the certificate in the issuing Certification Authority	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
issuer (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments/SEP Bulgaria JSC
	OU	SEP
	CN	SEP Root CA
validity	notBefore	UTC format
	notAfter	UTC format
subject (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign QES CA
	Street	1 Zlatovrah Str.
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Enhanced Key Usage		

Field Name	Value or limitation of value
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=eSign QES CA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/SEP_root_ca.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg

Field Name	Value or limitation of value
Basic Constraints	Subject Type=CA Path Length Constraint=None
Issuer Alternative Names	
Subject Alternative Name	
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	The Author's public key and algorithm to be used
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	CSP Electronic signature

XXIII. User Certificates

Users QES Certificates are issued by the Operational CA.

The period of validity of the issued Certificates is 3 (three) years.

The key length is 2048 bits for RSA algorithm or 163 bits ECDSA for algorithm.

1. eSign Qualified Private Profile

The Certificate type SEP Qualified Private is used to confirm the agreement / identity of an individual participating in the electronic exchange such as web-based applications, signature of electronic documents and / or contracts, banking transactions and making statements within the meaning of EDESA.

Statements are for and on behalf of the person.

Certificate eSign Qualified Private Profile:

Field Name	Value or limitation of value
version	Version 3
serialNumber	Unique serial number of the certificate in the issuing Certification Authority
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)

Field Name	Value or limitation of value	
issuer (Distinguished Name)	C	BG
	Street	1 Zlatovrah Str.
	L	Sofia
	O	System for Electronic Payments/SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign QES CA
validity	notBefore	UTC format
	notAfter	UTC format
subject (Distinguished Name)	*C	BG
	S	Author's area
	*L	Author's living place
	*OU	SEP Qualified Private
	*CN	Author's Name/Alias
	UID (0.9.2342.19200300.100.1.1)	EGNxxxxxxxxx[EGN/PNF/yymmdd of Holder]
	*E	Author's e-mail
	Street	Author's address
	Phone	Author's phone number
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	

Field Name	Value or limitation of value
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=This certificate is issued as qualified certificate for qualified electronic signature using secure signature creation device [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_QES_ CA.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier	
Subject Key Identifier	
Qualified Certificate Statements	Indicates that the certificate is issued as a certificate for qualified electronic signature

Field Name	Value or limitation of value
subjectPublicKeyInfo	The Holder 's / Author's public key and algorithm to be used
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
signatureValue	CSP Electronic signature

2. eSign Qualified Organization Profile

The Certificate type SEP Qualified Organization is used to confirm the agreement, or the identity of the entity participating in the electronic exchange such as web-based applications, signing of electronic documents and / or contracts, banking transactions and making statements within the meaning of EDESA.

The Holder and Author differ, as the Author is an individual, and the Holder – legal entity.

The author does the statements for and on behalf of the Holder.

Certificate eSign Qualified Organization Profile:

Field Name	Value or limitation of value	
version	Version 3	
serialNumber	Unique serial number of the certificate in the issuing Certification Authority	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
issuer (Distinguished Name)	C	BG
	Street	1 Zlatovrah Str.
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign QES CA
validity	notBefore	UTC format

Field Name	Value or limitation of value	
	notAfter	UTC format
subject (Distinguished Name)	*C	BG
	S	Author's working area for the Holder
	*L	Author's working place for the Holder
	O	Full name of the legal entity – Holder
	*OU	SEP Qualified Organization
	OU	Organizational unit of the Holder
	*CN	Author's Name/Alias
	T	Author's job position / empowerment
	OU	EIKxxxxxxxxxx[UCN of Holder] / other identification
	*E	Work e-mail of the Author for work correspondence
	Street	Author's work address
	Phone	Author's phone number
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	

Field Name	Value or limitation of value
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=This certificate is issued as qualified certificate for qualified electronic signature using secure signature creation device [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_QES_ CA.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier	
Subject Key Identifier	
Qualified Certificate Statements	Indicates that the certificate is issued as a certificate for qualified electronic signature

Field Name	Value or limitation of value
subjectPublicKeyInfo	The Holder 's / Author's public key and algorithm to be used
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
signatureValue	CSP Electronic signature

It is envisaged issuing of certificates with explanatory text "TEST" in the subject (Distinguished Name) field (without EGN / EIK) for cases requiring customization of systems for verifying QES SEP Organization. The purpose of such QES Certificates is only for testing.

3. eSign Qualified Profession Profile

The Certificate type SEP Qualified Profession is used to confirm the agreement / identity and professional affiliation of the person providing services or exercising a profession, while participating in electronic exchanges, such as web-based applications, signing of electronic documents and / or contracts , bank transactions and making statements within the meaning of EDESA.

The person is Holder and Author of the statements.

Statements are from and on behalf of the person.

Certificate SEP Qualified Profession Profile:

Field Name	Value or limitation of value	
version	Version 3	
serialNumber	Unique serial number of the certificate in the issuing Certification Authority	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
issuer (Distinguished Name)	C	BG
	Street	1 Zlatovrah Str.
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES

Field Name	Value or limitation of value	
	CN	eSign QES CA
validity	notBefore	UTC format
	notAfter	UTC format
subject (Distinguished Name)	*C	BG
	S	Holder 's area from registration address
	*L	Holder 's place from registration address
	O	Holder 's full name
	*OU	SEP Qualified Profession
	OU	Organizational unit of the Holder [profession, membership]
	UID (0.9.2342.19200300.100.1.1)	EGNxxxxxxxxx[EGN/PNF/yymmdd of Author]/other identification
	*CN	Author's name / alias
	T	Author's job position / empowerment
	OU	EIKxxxxxxxxx [UCN of Holder]/other identification
	*E	Work e-mail of the Author for work correspondence
	Street	Author's work address
	Phone	Author's phone number
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	
Certificate Policies	[1]Certificate Policy:	

Field Name	Value or limitation of value
	Policy Identifier=1.3.6.1.4.1.30299.2.5.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=This certificate is issued as qualified certificate for qualified electronic signature using secure signature creation device [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eSign.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_QES_ CA.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier	
Subject Key Identifier	
Qualified Certificate Statements	Indicates that the certificate is issued as a certificate for qualified electronic signature
subjectPublicKeyInfo	The Holder 's / Author's public key and algorithm to be used

Field Name	Value or limitation of value
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
signatureValue	CSP Electronic signature

It is envisaged issuing of certificates with explanatory text "TEST" in the subject (Distinguished Name) field (without EGN / EIK) for cases requiring customization of systems for verifying QES SEP Profession. The purpose of such QES Certificates is only for testing.

XXIV. Signing algorithm identifier

The field signatureAlgorithm contains the identifier of the algorithm used to create an electronic signature by the CA.

SEP Bulgaria uses the following algorithms:

- sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
- id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)

XXV. Electronic signature field

The value of the field SignatureValue is the result of hash function calculated in all fields of the Certificate and encrypted with the private key of the issuing CA of CSP.

XXVI. List with revoked certificates Profile

„List with revoked certificates“ (CRL) contains the following fields:

- tbsCertList: information about revoked certificates;
- signatureAlgorithm: identifier of the algorithm used for signing of „List with revoked certificates“;
- signatureValue: CA electronic signature, who issued „List with revoked certificates“.

The meaning of values in signatureAlgorithm and signatureValue is analogous to the electronic signature certificates.

The field TbsCertList field contains series of mandatory and optional fields. Mandatory fields identify the issuer of CRL, optional fields contain information about revoked certificates and CRL extensions.

The fields are as follows:

- version: version and format of CRL;
- signature: identifier of the algorithm used by CA issued the CRL;
- issuer: name of CA issued CRL. Each CA from SEP Bulgaria hierarchy issues separate CRL;
- thisUpdate: date of CRL publishing coded in UTC format;
- nextUpdate: notify for the date for next CRL publishing. If the field is available, its value indicates the latest date of publication. CRL renewal before that date is possible.

- revokedCertificates: „List with revoked certificates“, the field is empty if there are no revoked certificates. The information is contained in the following fields:
  - userCertificate: serial number of the revoked certificate;
  - revocationDate: the date certificate is revoked;
  - crlEntryExtensions: additional information regarding the revoked certificate.
- crlExtensions: additional information regarding CRL;
- AuthorityKeyIdentifier: allows identifying the public key corresponding to the private key used to sign the CRL;
- CRLNumber: contains a monotonically increasing sequence of numbers. Provides an easy way to determine when a CRL is replaced by another.
- Reasons for revocation:
  - unspecified: without specifying the reason for revocation;
  - keyCompromise: compromised private key;
  - cACompromise: compromised CA key;
  - affiliationChanged: updated Client data for Holder / Author;
  - superseded: certificate is renewed;
  - cessationOfOperation: Certificate is terminated;
  - certificateHold: Certificate is suspended;
- removeFromCRL: Certificate is reactivated.

„List with revoked certificates“ Profile

Field	Values	
version	Version 2	
issuer (Distinguished Name)	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP
	CN	{SEP Root CA, eSign QES CA}
	Street	1 Zlatovrah Str.
	E	esign@SEP.bg
thisUpdate	Date of CRL publishing	
nextUpdate	Date of next CRL publishing	
signature	Electronic signature of CRL issuer	
CRLNumber	Number from monotonically increasing sequence of numbers	

AuthorityKeyIdentifier		
revokedCertificates	userCertificate	Serial number
	revocationDate	Date of placement in CRL
	crlEntryExtensions	{unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn}

XXVII. SEP TSA profile

The time stamp certificate is signed by CSP electronic document, certifying the time of presenting an electronic signature created for a specific electronic document.

SEP TSA certificate is in compliance with RFC 3280, and requests and responses to SEP TSA for time verification are according to RFC 3161.

SEP TSA Certificate Profile:

Field	Value or limitation of value	
version	Version 3	
serialNumber	Unique serial number of the certificate in the issuing Certification Authority	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
issuer (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP QES
	CN	SEP Root CA
validity	notBefore	UTCTime format
	notAfter	UTCTime format
subject (Distinguished Name)	C	BG
	L	Sofia

Field	Value or limitation of value	
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES
	CN	SEP TSA
	E	esign@sep.bg
Key Usage	digitalSignature, nonRepudiation	
Enhanced Key Usage	timeStamping	
Certificate Policies	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice explicitText: SEP TSA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.sep.bg	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_root_ca.crl	
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg	

Field	Value or limitation of value
Basic Constraints	cA: no pathLenConstraint: 0
Issuer Alternative Names	
Subject Alternative Name	
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	The Holder 's / Author's public key and algorithm to be used
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	CSP electronic signature

XXVIII. OCSP profile

SEP Bulgaria provides the service for validation of issued certificates not only by access to CRL but also through online protocol for validation of the status of issued certificates - OCSP. In this case, SEP Bulgaria provides information about the status of all certificates issued in the hierarchy of SEP Bulgaria.

Удостоверението, с което се проверява онлайн отговора, се издава от SEP QES CA. eSign QES CA подписва със своя частен ключ резултата от проверката преди да го изпрати на потребителя. OCSP удостоверението е съгласно RFC 3280, а заявките и отговорите към eSign QES CA, за удостоверяване на статуса на издадено от СЕП България удостоверение, са съгласно RFC 2560.

The Certificate used for online validation is issued by eSign QES CA. eSign QES CA signs with its private key the validation result before sending it to the user. OCSP certificate is according to RFC 3280, and requests and responses to eSign QES CA, to validate the status of issued by SEP Bulgaria certificates are according to RFC 2560.

eSign OCSP Certificate Profile:

Name of Field	Value or limitation of value
version	Version 3
serialNumber	Unique serial number of the certificate in the issuing Certification Authority
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)

Name of Field	Value or limitation of value	
issuer (Distinguished Name)	C	BG
	Street	1 Zlatovrah Str.
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign QES CA
	E	esign@sep.bg
validity	notBefore	UTCTime format
	notAfter	UTCTime format
subject (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign OCSP
	E	esign@sep.bg
Key Usage	digitalSignature, nonRepudiation	
Enhanced Key Usage	OCSPSigning	

Name of Field	Value or limitation of value
Certificate Policies	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice explicitText: eSign OCSP [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_QES_ CA.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	cA: no pathLenConstraint: 0
Issuer Alternative Names	
Subject Alternative Name	
Authority Key Identifier	

Name of Field	Value or limitation of value
Subject Key Identifier	
subjectPublicKeyInfo	The Holder 's / Author's public key and algorithm to be used
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	CSP electronic signature

SEP Bulgaria includes in issued certificates in the Authority Information Access field information for the use of online validation on the status of issued certificates.

This User Guide has been prepared by SEP Bulgaria and approved by the Board of Directors with Resolution from 21.06.2013