



CERTIFICATION PRACTICE STATEMENT

Revision: 1.3

Spektar AD

11A Carnegie street

1000 Sofia, Bulgaria

phone: + 359 2 9699 200

fax: + 359 2 9699 255

<http://www.spektar.org>

CONTENT

1.1.1 Activities.....	5
1.1.2 Data on the provider.....	6
1.1.3 Contacts.....	6
1.2.1 Certification authority.....	7
1.2.2 Registration authority.....	7
1.2.3 Owner.....	8
1.2.4 Signatory.....	8
1.2.5 Relying parties.....	8
1.3.1 Content of certificates for electronic signature.....	8
1.3.2 Certificate use	9
1.3.3 Use of certificates outside given restrictions.....	10
2.1.1 Responsibilities of the CSPProvider.....	10
2.1.2 Responsibilities of the Owner and Signatory.....	11
2.1.3 Responsibilities of the trusting party.....	12
2.2.1 Responsibilities of the Certification services provider.....	13
2.2.2 Cases of non-liability.....	13
2.2.3 Responsibilities of the Owner and Signatory.....	14
2.3.1 Information published in the registry.....	15
2.3.2 Access to the information in the electronic registry.....	15
2.3.3 Updates of information in the registry.....	16
2.3.4 Security measures.....	16
2.4.1 Control by the Communications Regulation Commission.....	17
2.4.2 Audits of the information security system in the CSPProvider.....	17
2.5.1 Confidential information.....	18
2.5.2 Non-confidential information.....	18
2.5.3 Disclosure of information.....	18
2.6 Copyright.....	19
2.7 Termination of the activities of the CSPProvider.....	19
3.1.1 Types of names.....	20
3.1.2 Rules for entering names.....	20
3.1.3 Uniqueness of names	21
3.1.4 Procedure for deciding use of conflicting names.....	21
4.3.1 Conditions for certificate issuance.....	26
4.3.2 Who can submit an application for certificate issuance.....	26
4.3.3 Order for submission of applications for certificate issuance.....	26
4.3.4 Publishing the issued certificate	26
4.3.5 Acceptance of certificates by the Owner, Signatory, respectively.....	27
4.5.1 Reasons for certificate suspension	27
4.5.2 Who can apply for certificate suspension.....	27
4.5.3 Order for submission of application for certificate suspension.....	28
4.5.4 Notification of the Owner and Signatory.....	28
4.6.1 Reasons for renewal of suspended certificates.....	28
4.6.2 Who can apply for certificate renewal of suspended certificates.....	29
4.6.3 Order for submission of applications for certificate renewal of suspended certificates.....	29

4.7.1 Conditions for certificate renewal.....	29
4.7.2 Who can submit an application for certificate renewal.....	30
4.7.3 Order for submission of applications for certificate renewal.....	30
4.7.4 Acceptance of renewed certificates.....	30
4.8.1 Reasons for certificate revocation.....	30
4.8.2 Who can apply for certificate revocation.....	31
4.8.3 Order for submission of application for revocation of certificates.....	31
4.8.4 Checks in the certificate revocation list.....	31
4.8.5 Online status checks (OSCP).....	31
5.1.1 Layout and structure of operating teams.....	32
5.1.2 Premises.....	32
5.1.3 Physical access.....	32
5.1.4 Power supply and ventilation.....	33
5.1.5 Measures against flood.....	33
5.1.6 Anti-fire precautions.....	33
5.1.7 Duplicates of crucial information.....	33
5.2.1 General organization rules.....	34
5.2.2 Function distribution.....	34
5.3.1 Personnel qualification.....	34
5.3.2 Personnel training.....	34
5.3.3 Sanctions for breach of security rules.....	35
5.3.4 Outsourcing.....	35
5.3.5 Documentation presented to personnel.....	35
5.4.1 Types of recorded events.....	35
5.4.2 Frequency of recording.....	36
5.4.3 Keeping period of the reports.....	36
5.4.4 Report protection.....	37
5.4.5 Procedures for keeping reports.....	37
5.4.6 System for keeping data from security assessments.....	37
5.4.7 Notification of persons causing the events.....	37
5.4.8 Vulnerability assessment.....	37
5.5.1 Types of events recorded.....	37
5.5.2 Keeping period of the archives.....	38
5.5.3 Archive protection.....	38
5.5.4 Procedures for archive keeping.....	38
5.6.1 Damage to computer resources, software and/or information.....	39
5.6.2 Recovery from crises.....	39
5.6.3 Disclosure of keys.....	40
6.1.1 Generation of the private-public key pair of the Certification Authority Spektar Root CA.....	42
6.1.2 Generation of the private-public key pairs of the Certification Authorities Spektar Universal CA and Spektar NonUniversal CA.....	43
6.1.3 Generating a private-public key pair for users' certificates.....	43
6.1.4 Submission of private keys.....	44
6.1.5 Providing public keys by the Owner/Signatory to the CSPProvider.....	44
6.1.6 Providing public keys to the Certification Authorities of interested persons.....	45
6.1.7 Key length.....	45
6.1.8 Application of keys (according to KeyUsage field).....	45
6.2.1 Standard for cryptographic modules.....	45

6.2.2 Keeping and control of private keys	46
6.2.3 Input of keys in crypto-modules	46
6.2.4 Methods for deactivation of private keys.....	46
6.2.5 Methods for deactivation of private keys.....	47
6.2.6 Method for destruction of private keys.....	47
6.3.1 Public keys archive.....	47
6.3.2 Validity period of certificates.....	48
7.1.1 Version of issued certificates	50
7.1.2 Extensions of issued certificates	50
7.1.3 Algorithm for signing certificates issued by the CSProvider.....	51
7.1.4 Form and restrictions for names used.....	51
7.1.5 Identification of the policies for certificate issuance.....	51
7.2.1 Profile version.....	52
7.2.2 Codes for suspension and revocation of certificates.....	52
8.2.1 Compulsory insurance.....	54
8.2.2 Insurance coverage	54
8.4.1 User's Manual distribution.....	55
8.4.2 Updates of the User's Manual	55

1. Introduction

This document contains the practice followed by Spektar AD in its capacity of a certification services provider (in short CSProvider) for certification services which includes but is not limited to issuance, suspension, revocation and renewal of certificates in accordance with the particular requirements of the policies for the different certificates.

The *Certification Practice Statement* is part of the *User's Manual*, developed in accordance with the requirements of: RFC2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" , RFC3238 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", as well as „Designing and managing a Windows[®] Public Key Infrastructure”.

The Certification Practice Statement has the effect of general rules and regulations for certification services offered by the CSProvider

1.1 Spektar AD as a certification services provider

1.1.1 Activities

The certification services provider Spektar AD runs its business on certification services provision through specially created within the framework of the legal person organizational structure *Certification Services Team*.

The activities of the CSProvider on certificate issuance under article 24 of the EDESA an keeping a registry of them include:

- issuance and signing of certificate based on established identity and valid data of the Owner/Signatory;
- publishing the issued certificates in an electronic registry;
- management of the issued certificates including suspension, renewal, extension and revocation of certificates;
- maintenance and security measures for the electronic registry;
- publishing certificate revocation lists in the registry;
- giving any third party access to the certificate revocation lists observing the requirements of article 28.2 of the EDESA.

Detailed description of the services offered by the CSPProvider can be found in the *Certificate Policy* (Section 2).

1.1.2 Data on the provider

SPEKTAR AD is registered under company case No59009/1990 according to the list of the Sofia City Court with main office and management address: Sofia, Sredetz, 11A Carnegie street, BULSTAT: 831431323, VAT:BG831431323

1.1.3 Contacts

Postal address:

Registration Authority

Spektar AD

11A Carnegie street

1000 Sofia, Bulgaria

phones: + 359 2 9699 200 – information
+ 359 2 9699 252 – registration authority
+ 359 2 9699 256 – technical support

fax: + 359 2 9699 255

website:

<http://www.spektar.org>

Electronic mail addresses:

ca@spektar.org

info@spektar.org

tech@spektar.org

delovodstvo@spektar.org

1.2 Parties involved in issuance and use of certificates

1.2.1 Certification authority

Certification authority is a term covering all objects, parts of the structure of the CSProvider which sign, publish and change the status of the certificates.

The Certification authority functions through a separate team in the organizational structure of the CSProvider.

There are the following separate *Certification authorities* in the infrastructure of the CSProvider:

- Spektar Root CA (Level 0) – issues certificates for subordinate Certification authorities in the *Spektar* domain (Spektar Universal CA and Spektar NonUniversal CA);
- Spektar Universal CA (Level 1) – issues users' certificates of the *Universal* and *Restricted* types in accordance to the *Certificate Policy*;
- Spektar NonUniversal CA (Level 1) – issues users' certificates of the *NonUniversal* type in accordance with the Certificate Policy.

1.2.2 Registration authority

The registration authority is an object with the following functions:

- identification and establishing of authenticity of the information when applications for certificate issuance are received;
- verification of the validity of submitted electronic application for certificate;
- initiation and transfer to the Certification authority of requests for suspension, renewal or revocation of issued certificates;
- approval of applications for extension of validity of certificates on behalf of the CSProvider.

The *Registration authority* functions through a separate team in the organizational structure of the

CSPProvider.

Third parties, which in future will have contractual relations with the CSPProvider can function as Registration authority and permit the issuance of the *Spektar Universal Certificate* certificates. These third parties shall observe all conditions in *Certification Practice Statement* and *Certificate Policy*.

1.2.3 Owner

The Owner is a physical or legal person on behalf of whom electronic statements are signed and is stated in the issued certificate for electronic signature as the Owner.

1.2.4 Signatory

The Signatory is a physical person who creates and signs electronic statements on behalf of the Owner in accordance to the representative powers given him.

1.2.5 Relying parties

The relying parties are physical or legal persons – addressees of electronic statements signed with electronic signature for which there are issued by the CSPProvider certificates for electronic signature.

After checking all circumstances regarding validity of the signature according to the rules in Section 2.1.3 the addressee of the electronic statement signed with electronic signature of the Owner shall trust and accept that the signature has the legal value of a handwritten signature.

1.3 Use of certificates for electronic signature

The certificate for electronic signature is an electronic document signed by a certification services provider who verifies the relation between Owner/Signatory and a private key possessed by him. The certificate is used for identification and personal identification of the Owner/Signatory in cases such as: signing of electronic documents, access to information systems or encipherment of information.

1.3.1 Content of certificates for electronic signature

Certificates for electronic signature issued and signed by the CSPProvider contain:

- the public key of the private-public key pair, which corresponds to the certificate;
- information about the certification authority issued and signed the certificate;
- information about the Owner – its type depends on whether the Owner is a physical or legal person;

- information about the Signatory, including information for his empowerment by the Owner in cases when the Owner and the Signatory are not the same person;
- validity period of the certificate;
- date and time of issuance;
- restrictions imposed on the certificate;
- references to the certificate of the *Certification authority* signed the certificate;
- identifier of the algorithm for electronic signature defining the algorithms used for generation of the key pair and advanced electronic signature;
- unique serial number of the certificate;
- responsibilities and warranties of the provider;
- reference to the registration of the provider in the Communications Regulation Commission.

The content of each particular certificate is described by its profile. Information on the profiles of the certificates issued by the CSPProvider can be found in Section 7 of this document and in the respective issuance policy which is part of the *Certificate Policy*.

1.3.2 Certificate use

According to the X.509 specification the certificate and corresponding private-public key pair can have different applications some of which are:

- Digital Signature – to prove the integrity of the data in the signed electronic document, to prevent the document from changes and to show the connection between the document and the Signatory;
- Non-Repudiation – to establish the identity of the Signatory of the digital signature;
- Key encipherment – for exchange of keys used for data encipherment;
- Data encipherment – for transmitting data through insecure communication carrier and for archiving.

The following table describes in short the purposes of the certificates and their respective possible application.

Purpose of the certificate	Application of the certificate
Signing (Signature)	Data signing, authentication, non-repudiation
Encipherment (Encipherment)	Data encipherment & deencipherment
Signing and Encipherment (Signature и Encipherment)	Data encipherment & deencipherment, digital data signing, authentication

The application of each particular certificate issued by the CSPProvider is described in the certificate issuance policy in the *Certificate Policy*.

1.3.3 Use of certificates outside given restrictions

When the certificate is issued with written restrictions regarding its application it can not be used outside these restrictions.

The CSPProvider is not responsible for uses of certificates outside their written restrictions.

2. General provisions

2.1 Responsibilities

2.1.1 Responsibilities of the CSPProvider

The CSPProvider has the following responsibilities

- to maintain available means which provide the infrastructure of the certification services (PublicKeyInfrastructure), archives and website with possibility to act in accordance with the requirements of the Electronic Document and Electronic Signature Act (EDESA);
- to be insured for the time of its business as a certification service provider against damages due to failure to fulfill its responsibilities under the EDESA and sublegislation on its application;
- to have technical equipment and technology which assure reliability of the systems used and cryptographic security of the signatures created through the processes run by these equipment and technology;
- to maintain personnel with the necessary expert knowledge, experience and qualifications, especially in the field of the technology of advanced electronic signatures, as well as good knowledge of the security procedures;
- to provide possibility for the precise defining of the time of issuance, suspension and renewal of certificates;
- to provide measures against forgery of certificates and confidentiality of the data to which there is access during creation of signature;
- to use reliable systems for keeping and management of certificates which make sure that:
 - only duly authorized officials to have access to making changes;
 - authenticity and validity of certificates is established;
 - there is a possibility for restricted access to published certificates;

all technical problems related to security are immediately reported to supporting personnel;

the possibility for confirmation of the private keys is terminated with validity expiry.

- to allow immediate suspension and revocation of certificates;
- to issue a certificate upon request by any person, informing him ahead of the participation in organizations for voluntary accreditation and registration by the Communications Regulation Commission;
- to inform persons applying for certificates about the conditions for issuance and application of the certificate, including restrictions in use and procedures for submitting claims and conflict solving;
- when issuing certificates to check the authenticity, respectively identity of the Owner/Signatory of the universal electronic signature using allowed means and if necessary other data on the persons included in the certificate;
- to publish the issued certificate in a way that allows third parties to have access to it in accordance with the directions given by the Owner;
- to not keep or copy data on the creation of private keys;
- to immediately take actions related to the suspension, renewal and revocation of certificates when respective reasons for that are present;
- to inform the Owner and/or Signatory about any circumstances regarding validity or reliability of the issued certificate;
- to possess universal electronic signature which to be used only in relation to its activities as a certification services provider;
- to observe its company and public policies and procedures;
- to observe operating legislation.

2.1.2 Responsibilities of the Owner and Signatory

The Owner and Signatory stated in the certificates issued by the CSPProvider have the following responsibilities:

- to read and observe the conditions and rules when receiving certification services from the CSPProvider, present in this document, the *Certificate Policy* and the rest of the documents published in the electronic registry;
- to give true, precise and full information required by the CSPProvider in accordance with the legislation and this document and the respective policies for submission of application for issuance and management of certificates;

- to generate the key pair using a secure method and algorithm in accordance to the Ordinance for requirements for algorithms for advanced electronic signature;
- to check that the content of the DN (information given by him for certification) is complete and true. In case of any discrepancies in the information given and the content of the DN to inform the CSPProvider immediately;
- to stop using the certificate in case of doubt for discredit of the private key and submit an application for suspension to the CSPProvider;
- to stop using the certificate in case of loss or discredit of the private key of the issued certificate and immediately inform the CSPProvider about changed circumstances;
- to stop using the certificate in cases of old, changed, incorrect or wrong information, included in the issued certificate and submit an application for certificate revocation;
- to change his PIN for access to the smart card where the private key is kept before using the certificate;
- to take all necessary measures for prevention from discredit, loss, disclosure, modification or other unauthorized use of the private key corresponding to the public key published in the certificate;
- to use the issued by the CSPProvider certificate only for legal purposes and in accordance with the policy and practice for certification services provision.

2.1.3 Responsibilities of the trusting party

The trusting party is obliged to check the validity of the certificate which accompanies the electronic statement by the Owner/Signatory.

To check the validity of the certificate the Trusting party is obliged to:

- make a reference with the certification revocation lists published in the electronic registry of the CSPProvider in accordance with the rules stipulated in Section 2.4 of this document;
- to make a reference for validity of the whole chain of certificates to the basic certificate of the CSPProvider (Spektar Root CA).

After checking all circumstances concerning the validity of the signature the Trusting party of an electronic statement signed with the electronic signature of the Owner shall trust and accept that the signature has the legal value of a handwritten signature.

Checks of circumstances concerning validity of the signature include verifying of the following:

- the certificate is used properly regarding application and purpose and in accordance with the issuance policy;
- the algorithms used for generation of the private-public key pair meet the security requirements of the trusting party;
- the length of the keys used complies with the security requirements of the Trusting party;
- time of electronic signing and respectively establishing the validity of the certificate at this moment.

The CSPProvider is not responsible for any damages to the Trusting party due to failure to make the checks described above.

2.2 Responsibilities

2.2.1 Responsibilities of the Certification services provider

The CSPProvider is responsible for the checks of identity and personal identification of the subjects applying for certificates and for the actions of its Registration Authorities.

The CSPProvider is responsible all procedures for provision of certification services to be run in accordance with the rules in the *Certification Practice Statement* and *Certificate Policy*.

The CSPProvider is responsible before the Owner and all third parties for damages due to:

- failure on the part of the CSPProvider to meet the requirements for the activities of the certification services providers stipulated in article 21 of the EDESA;
- failure on the part of the CSPProvider to meet the requirements for the activities of the certification services providers stipulated in article 22 of the EDESA;
- failure on the part of the CSPProvider to meet the requirements for the activities of the certification services providers stipulated in article 25 of the EDESA;
- incorrect or missing data in the certificate at the moment of issuance;
- at the moment of issuance the person stated as Owner did not have the private key corresponding to the public key;
- any discrepancies in data for establishing use of the private key and data given by the person using the public key.

2.2.2 Cases of non-liability

The CSPProvider is not liable in cases when occurred damages are due to negligence, failure to fulfill duties or lack of knowledge in the field of PKI technologies on the part of the Owners, Signatories or Relying parties.

The CSPProvider is not liable for damages due to:

- use of certificate outside the prescribed use and restrictions;
- illegal actions by the Owner, Signatory or third parties;
- use of certificates which were not issued in accordance with the procedures in the *Certification Practice Statement* and *Certificate Policy*;
- use of void certificates – suspended, revoked or with expired validity;
- untimely suspension or revocation of certificates due to application forgotten by the Owner/Signatory or due to reasons outside the control of the CSPProvider (natural disasters and incidents);
- discredited private key corresponding to the public key in the certificate;
- quality and functionality of software products and hardware devices used by the Owner, Signatory or the Relying parties.

2.2.3 Responsibilities of the Owner and Signatory

The Owner is responsible before the conscientious third parties when at the generation of the private-public key pair the algorithm used does not meet the requirements of the ordinance for algorithms for advanced electronic signature.

The Owner is responsible before conscientious third parties if the Signatory:

- does not meet the security requirements determined by the certification services provider Spektar Org®;
- does not request from the CSPProvider to suspend the certificate when he has found out that the private key had been used improperly or there is a risk of improper use of the private key.

The Owner who has accepted the certificate at its issuance is responsible before third parties:

- if the Signatory is not authorized to hold the private key corresponding to the public key stated in the certificate;
- for incorrect statements before the CSPProvider related to the content of the certificate.

The Signatory who has accepted the certificate at its issuance is responsible before conscientious third parties if he was not authorized to apply for the certificate.

The Owner, Signatory, respectively, is responsible before the CSPProvider if he had accepted a certificate issued by the CSPProvider based on incorrect data given by the Owner/Signatory or based

on data concealed by the Owner/Signatory.

2.3 Electronic registry

2.3.1 Information published in the registry

The certification services provider CSPProvider keeps an electronic registry in which it publishes:

- the basic certificate of the CSPProvider (Spektar Root CA);
- the operating certificates of the Certification Authorities (Spektar Universal CA and Spektar NonUniversal CA);
- all certificates issued by the CSPProvider;
- certificate revocation lists (CRL).

The following is also published in the electronic registry:

- *Certification Practice Statement*;
- *Certificate Policy*;
- *User's Manual*, containing the Policy and Practice for certification services:

conditions and order for issuance and management of certificates;

rules for establishing the identity of the Owner and Signatory of universal electronic signatures;

responsibilities of the certification services provider, Owner, Signatory and relying party;

security measures applied by the CSPProvider in its capacity as a certification services provider.

- rules and order for use of the universal electronic signature and requirements for the private key;
- financial conditions for the certification services provision by the CSPProvider;
- additional information in accordance with the requirements of the EDESA.

2.3.2 Access to the information in the electronic registry

The CSPProvider offers directory services for the information kept in the electronic registry in accordance with the X.500 recommendations providing access to the information via LDAP protocol and everybody interested can be given a reference through a suitable web client.

The electronic registry is public and the CSPProvider can not restrict access to the information in it.

Every interested person has the right:

- of access to read the published documents;
- of access to read the basic and operating certificates of the CSPProvider (Spektar Root CA, Spektar Universal CA and Spektar NonUniversal CA);
- to search issued valid certificates by certain attributes such as name of Owner or Signatory, electronic mail address, serial number.

Access to a particular valid certificate in the registry can be restricted only upon expressed wish of the Signatory in the application form.

The information published in the electronic registry of the CSPProvider is constantly accessible apart from cases of events outside the control of the provider or catastrophic and/or disastrous circumstances.

2.3.3 Updates of information in the registry

The certificates issued by the CSPProvider are published in the electronic registry immediately after their signing by the Certification Authority.

Updates of certificate revocation lists are done in every 3 /three/ hours. The lists are published right after each update.

All changed revisions of the Certificate Policy and Certification Practice Statement are published immediately after each approved change in accordance with the rules stipulated in Section 8.4 of this document.

2.3.4 Security measures

The CSPProvider ensures the security of the electronic registry with the implemented information security system corresponding to the requirements of the ISO 17799 standard.

In accordance with the information security system functioning in the CSPProvider measures are taken regarding logical access to the information in the registry and physical access to the computer information systems keeping the data. The measures taken render changes in data possible and risk of unauthorized use is brought to a minimum.

Only duly authorized officials of the CSPProvider can update and input information in the electronic registry.

2.4 Control over the CSPProvider's activities

2.4.1 Control by the Communications Regulation Commission

According to the rights of the Communications Regulation Commission stipulated in article 32 of the EDESA it controls the activities of the CSPProvider. This control includes:

- control on reliability and security of the services offered by the CSPProvider;
- approval of the policy and practice for the certification services offered by the CSPProvider, as well as of procedures and security measures.

Representatives of the Communications Regulation Commission has the right:

- of free access in accordance to the Information security Policy to the buildings and premises in which the CSPProvider offers certification services;
- to check the qualification documents of the CSPProvider's employees;
- to request information and documents related to internal control.

Control is exercised by officials of the Communications Regulation Commission or by persons under article 32.3 of the EDESA who can run full checks on the certification services provision.

2.4.2 Audits of the information security system in the CSPProvider

The CSPProvider has implemented and uses a system for the management of the information security in accordance to the requirements of the ISO 17799 standard. The system covers the aspects of information security for the certification services provision by the CSPProvider.

According to the internal rules and procedures of the CSPProvider regular audits are run aiming to:

- discover any deviations from the accepted rules and procedures;
- prevent events which could have negative impact on information security;
- outline possible ways to improve security.

The conclusions of the auditors are discussed in the Council for information security in the CSPProvider. The Council gives recommendations regarding the importance of the discrepancies found.

In case the discrepancies found are an immediate threat for the information security in the CSPProvider in 30 /thirty/ days period of time an action plan is developed and realised in a reasonable

period of time.

2.5 Confidentiality of information

2.5.1 Confidential information

Personal data of the Owner and Signatory of certificates which are collected in the processes of application, issuance and management of the certificates and are not published in the issued certificate are confidential.

The CSProvider considers confidential the information in:

- certification services contract;
- applications for certificates;
- journals of the operating activities of the information systems of the CSProvider;
- records of payments;
- internal rules and procedures of the information security system of the CSProvider;
- action plans for unforeseen cases and recovery from disasters.

2.5.2 Non-confidential information

Personal data of the Owner and Signatory which is published in the fields of the issued certificates is considered non-confidential.

When signing a contract for certification services with the CSProvider the Owner and Signatory agree that the personal data necessary for the issuance of the certificate will be accessible by third parties via their publication in the electronic registry of the provider.

Everybody can access information published in the electronic registry relating to:

- certificates issued by the CSProvider;
- certification revocation lists;
- Policy and Practice for the certification services offered by the CSProvider;
- other documents such as rules for the use of electronic signature, prices for the services offered by the CSProvider etc.

2.5.3 Disclosure of information

The confidential information collected and kept by the CSProvider can be disclosed in the following cases:

- the Owner or Signatory of a certificate can give written permission to the CSProvider to present to third parties their personal data collected during the process of issuance and management of the certificate;
- before persons and organization which have legal rights to access confidential information.

2.6 Copyright

The CSProvider has the copyright on the issued certificates and certificate revocation lists. Owners and Signatories can use and copy the certificates given to them providing:

- the integrity of the information present in the certificate is kept;
- certificates are used properly for the purposes described in the issuance policy of the CSProvider.

The CSProvider has the copyright on the *Certificate Policy* and *Certification Practice Statement*, published in the electronic registry of the provider and constituting the *User's Manual*.

The CSProvider retains all rights on possessed trademarks and names present in the fields of the issued certificates.

Owners/Signatories retain all right on possessed trademarks and names present in the fields of the issued certificates.

The Owner/Signatory has the rights on the private-public key pair which corresponds to the issued certificate.

The Owner/Signatory has the rights on the means for activation of the private key.

2.7 Termination of the activities of the CSProvider

When terminating its business the CSProvider runs the following procedure stipulated in the ORDINANCE on the Activities of Certification-Service-Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services:

- The CSProvider informs the Communications Regulation Commission and the users for its intention 4 months before termination date the latest;
- regardless of the previous action the CSProvider is obliged to inform immediately the

- Communications Regulation Commission in case of insolvency claim, declaring nullity of the organization or other claims for termination or liquidation;
- before terminating its business the CSPProvider is obliged to do everything necessary to provide the duration of the validity of the certificates issued by it;
 - exercising the previous point the CSPProvider shall inform in written the Communications Regulation Commission and users whether another registered certification services provider will continue to manage the certificates and announce its name at the moment of termination of business the latest;
 - in case the activities of the CSPProvider will be taken by another registered certification services provider under article 43 of the ORDINANCE on the Activities of Certification-Service-Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services:

The CSPProvider informs its users about the conditions for management of the certificates transferred to the new provider;

The CSPProvider duly transfers all documentation related to its activities to the new registered provider.

- in case the CSPProvider has not transferred its business to another registered provider, the issued certificates are revoked. In such case the CSPProvider gives its documentation to the Communications Regulation Commission immediately after termination.

The Communications Regulation Commission maintains a registry of the revoked certificates of the terminated certification services provider.

3. Identification and certification of the authenticity of information

3.1 Use of names

3.1.1 Types of names

The name and marks which help individualize the Owner and Signatory in the respective fields of every type of certificate are formed according to the X.500 recommendations and the policy for the issuance of the respective type of certificate.

3.1.2 Rules for entering names

The certificates contain the names of the Owners and Signatories subjects of the certificates issued.

Entering the names in the fields of the certificates shall follow the rules described in Section

7 (Profile of certificates issued) of the *Certification Practice Statement*.

There is a description of the name field content for the different certificates issued by the CSPProvider in the policy for issuance and management of the particular certificate which is part of the *Certificate Policy*.

3.1.3 Uniqueness of names

The CSPProvider guarantees that the names entered in the DN (Distinguished Name) field for each Owner and Signatory are unique.

The uniqueness of the names is guaranteed by the automated processing of the application forms for certificates which allows the finding of conflicts at the stage of entering data for the certificates before their issuance.

The CSPProvider allows issuance of more than one certificate with the same value in the DN (Distinguished Name) field providing that the name belongs to the same physical or legal person.

3.1.4 Procedure for deciding use of conflicting names

Owners and Signatories do not have the right to apply for certificates using names which violate somebody's substantial or unsubstantial rights.

The CSPProvider is not responsible for cases when names used in certificate violate someone else's rights on trade name, trademark, domain, copyright, etc.

In cases of conflicts regarding use of names the CSPProvider reserves the right not to issue a certificate.

3.2 Certification of identity of a physical person

The establishment and check of the identity of the physical person – Owner/Signatory is done by the Registration Authority.

To establish and check the identity of a physical person he has to present an identity document. The copy of the personal identity card with the **line 'I agree this copy of my personal identity card to be used for the purposes of the CSPProvider.'** on it, signed in hand by the physical person, remains in the archive of the CSPProvider.

The physical person applying for a certificate or does some activities for the management of the issued certificate, duly fills in and submits to the Registration Authority, accordingly to the policies of the CSPProvider for issuance and management of the different certificates.

The filled in documents contain data on the person, including phone numbers for contact, address of residence and e-mail. The physical person confirms these data in the application documents by:

- handwritten signature on the documents before an authorized employee of the Registration Authority when documents are handed in personally;
- notarizing the document sent to the Registration Authority by mail.

The CSPProvider runs checks for the authenticity of the information in the filled in documents which include checks for Personal Identification Number (as well as indication of its nationality) validity of the person and correspondence between data for the certificate and data in the person's identity documents.

A list of the documents requested from a physical person applying for issuance and management of a certificate can be found in *Certificate Policy (Section Rules for issuance and management of certificates)*.

3.3 Identification of legal persons

The identity of an organization/trader – Owner is established by the Registration Authority.

The presentation of the following is needed to identify an organization/trader:

- a court decision or another document of creation;
- Bulstat;
- VAT number;
- VAT registration, if applicable;
- current state document.

A list of the requested documents can be found in the policy for issuance and management of the specific certificate. Copies of all requested documents remain in the archive of the CSPProvider.

The person representing the organization certifies the authenticity of the information given in the documents through:

- 'True with the original' line, a seal of the organization and signing by hand the documents before an authorized employee of the Registration Authority in case he submits the documents in person;
- Notarizing the documents he sends to the Registration Authority my mail.

The identity of the Signatory (the person representing the organization) is certified according to the rules in Section 3.2. and his representative powers according to the rules in Section 3.5.

The registration Authority runs checks for the authenticity of the information given in the documents including:

- verification at the notary public;

- electronic registers (SIELA, APIS, DELFI);
- verification at the local/state authorities.

3.4 Certifying possession of the private key

To issue or extend a certificate the CSPProvider has to receive an electronic application in PKCS#10 format. The specification of this format application for certificate requires it to be signed by the Signatory who possesses the private key.

The CSPProvider runs checks for validity of the electronic signature accompanying the application. This check of signature validity is in accordance with article 17 of the EDESA.

Established validity of the electronic signature is sufficient to consider that the Signatory who submitted the application possesses the private key which is technically fit and corresponds to the public key in the application.

When the Signatory downloads an issued or extended certificate from a distance a check for possession of the private key is run, using a specialized software product developed by the CSPProvider. The mechanism of this check is based on electronic signing of documents. Checks for signature validity in this case are run in accordance with article 17 of the EDESA and the ORDINANCE on the Activities of Certification-Service-Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services.

3.5 Confirmation of representative powers

In case the application for issuance or management of a certificate is not submitted by the Owner, we request a notarized letter of attorney by the Owner with which he authorizes the Signatory to:

- represent the Owner before the CSPProvider in matters relating to the services of the latter in its capacity of a certification services provider;
- take all necessary actions for the issuance and management of certificates in the meaning of articles 24 and 33 of the EDESA

The letter of attorney from the previous point is notarized and presented to the Registration

authority by an authorized person.

3.6 Identification and establishing authenticity of information in cases of changed private-public key pair

The private-public key pair can be changed in cases when the Owner wants to prolong the certificate and submits an application for that before the expiry date. In such cases the CSProvider recommends generation of a new key pair in order to avoid risk of discredit of the old pair.

The procedure for identification and establishing identity in cases of applications for renewal of certificate with change of the private-public key pair includes:

- establishing identity of the person submitted the application – done in accordance with the rules described in Section 3.2;
- in case the person submitted the application is not the Owner his representative powers are confirmed – done in accordance with the rules described in Section 3.5;
- certifying possession of the private key by the applicant – done in accordance with the rules described in Section 3.4.

3.7 Identification and establishing authenticity of information in cases of applications for revocation of certificates

In accordance with article 27.2 of the EDESA the CSProvider is obliged to check the identity and representative powers of the person who applies for revocation of a certificate.

To establish the identity of the person applied for revocation of a certificate the rules described in Section 3.2 are applied.

In case the person who applied for certificate revocation is not the Owner or Signatory the CSProvider applies the rules for confirmation of representative powers described in Section 3.5

4. Operating rules for issuance and management of certificates

4.1 Submission of application for a certificate

Application for certificate issuance can submit:

- any physical person who wishes to receive personal certificate;

- any representative of an Organization/Trader in his capacity of Signatory who is duly authorized to do that.

The applicant has to sign a contract with the CSProvider regulating relations between the parties and follow the steps of the following procedure:

- to fill in the documents according to the CSProvider's issuance policy for the particular type of certificate and give true and correct information;
- to generate the key pair observing the security requirements stipulated in the EDESA and the CSProvider's issuance policy for the particular type of certificate;
- to give his public key to the CSProvider by forming an electronic application in PKCS#10 format;
- to verify the possession of the private key which together with the given to the CSProvider public key comprise an asymmetric cryptographic pair.

4.2 Processing applications for certificate issuance

The CSProvider runs checks on the identity of the applicant authenticity of the presented information according to the rules and procedures in Section 3.2.

When the request for certificate issuance is satisfied the CSProvider requires confirmation of the content of the requested certificate by the Owner, Signatory, respectively.

The CSProvider changes the content of the requested certificate if the Owner or Signatory point out any discrepancies or omissions related to the information given by them.

The Owner/Signatory confirms the changes made by the CSProvider.

In cases of negative results from the procedures on all checks for authenticity of information the CSProvider refuses to issue a certificate and informs the applicant for the reasons.

Unsuccessful applicants have the right to submit new applications.

4.3 Issuance and publishing of certificates

4.3.1 Conditions for certificate issuance

The CSPProvider issues a certificate upon written request by the Owner. The request is satisfied if:

- the information about the Owner presented to be included in the certificate is true and complete;
- the private key:
 - is held by the Owner;
 - is technically fit to be used for the creation of universal electronic signature;
 - corresponds to the public key so that through the public key is possible to verify that a particular electronic signature is created with the private key.

In case the requested certificate is for universal electronic signature with Signatory different from the Owner the request is satisfied providing the above-stated conditions are met and:

- information about the Signatory presented to be published in the certificate is also true and complete;
- the private key is held by the Signatory.

4.3.2 Who can submit an application for certificate issuance

Only the Owner or a duly authorized by him person (Signatory) can submit an application for certificate issuance.

4.3.3 Order for submission of applications for certificate issuance

The order for submission of applications for issuance of a certificate by the CSPProvider and the issuance procedure are described in the issuance and management policy for the particular type of certificate which is part of the *Certificate Policy*.

4.3.4 Publishing the issued certificate

The CSPProvider publishes the issued certificate in the public electronic registry after the certificate is signed by the Certification authority.

4.3.5 Acceptance of certificates by the Owner, Signatory, respectively

Issued and renewed certificates are accepted in accordance with the rules in Section 4.4

4.4. Acceptance of certificates

The Owner or Signatory can in a period of 3 /three/ days after the loading and installment of the certificate make a claim for incorrect content.

If after this period of time the Owner/Signatory has not made any claims about the correctness of the content the certificate is considered finally accepted.

The certificate is considered finally accepted by the Owner and Signatory if before the 3 /three/ day's period of time after its issuance it is used at least once.

The rules stipulated here are applicable for both issuance and renewal of certificates.

4.5 Certificate suspension

4.5.1 Reasons for certificate suspension

The CSPProvider suspends the certificate for the necessary period of time regarding circumstances but for no longer than 48 hours if there is a reason to believe that the certificate should be suspended.

The CSPProvider considers reasons for termination:

- lost/stolen smart card;
- employee has left the company;
- change of certified data about the Owner or Signatory in the certificate;
- suspicion that the certificate has been compromised;
- other.

4.5.2 Who can apply for certificate suspension

The CSPProvider suspends a certificate issued by it for the necessary regarding circumstances period of time, but for no longer than 48 from the suspension moment:

- upon request by the Owner or Signatory with no obligation to check the identity or representative powers;
- upon request by a person who because of circumstances is clear to know about any breach of the security of the private key such as representative, partner, employee, family member, etc.

In cases of immediate danger for the interests of third parties or in presence of sufficient data on breach of the law, the Chairman of the CRC can oblige the CSPProvider to suspend the certificate for the period of time needed regarding circumstances but for no longer than 48 hours from the suspension moment.

4.5.3 Order for submission of application for certificate suspension

The order for submission of applications for suspension of a certificate issued by the CSPProvider is described in the issuance and management policy for the particular type of certificate which is part of the *Certificate Policy*.

Certificates are suspended by putting them in the Certificate Revocation List and publishing the updated list in the electronic registry of the provider according to Section 2.4.

4.5.4 Notification of the Owner and Signatory

The CSPProvider immediately informs the Owner and Signatory about the certificate suspension.

4.6. Renewal of suspended certificates

4.6.1 Reasons for renewal of suspended certificates

Suspended certificates are renewed:

- after the maximum period of suspension of 48 hours if no application for certificate revocation has been received meanwhile;
- before the maximal suspension period of 48 hours if the reason for suspension is cleared or the Owner applies for a renewal after the CSPProvider or the Communications Regulation Commission are assured that the Owner is informed of the reason for suspension and the application for renewal is submitted on the basis of this finding.

4.6.2 Who can apply for certificate renewal of suspended certificates

Only the Owner or a duly authorized by him person can submit an application for renewal of a suspended certificate.

4.6.3 Order for submission of applications for certificate renewal of suspended certificates

The order for submission of applications for renewal of a suspended certificate is described in the issuance and management policy for the particular type of certificate which is part of the *Certificate Policy*.

4.7 Certificate renewal

Owner's certificates which are not revoked can be renewed before their validity expires without the need to generate a new key pair.

When renewing a certificate it is possible to regenerate the private-public key pair (re-key) or to issue the certificate for the current pair.

The CSProvider recommends keeping the initial key pair only for the first renewal in order to reduce the risk of key discredit.

4.7.1 Conditions for certificate renewal

A certificate issued by the CSProvider can be renewed providing:

- there is no change in the initially given information about the Owner and Signatory, certified with the current certificate;
- the certificate has not expired;
- the certificate is not revoked;
- an application for renewal is submitted no earlier than 30 /thirty/ days and no later than 10 /ten/ days before the expiry date of the certificate.

If one of the conditions in the previous point is not met the rules for issuance of a new certificate according to Section 4.3 are followed.

4.7.2 Who can submit an application for certificate renewal

Only the Owner or a duly authorized by him person can submit an application for certificate renewal.

4.7.3 Order for submission of applications for certificate renewal

The order for submission of applications for renewal of a certificate issued by the CSProvider and the renewal procedure are described in the issuance and management policy for the particular type of certificate which is part of the *Certificate Policy*.

The corresponding policy contains a description of the certificate renewal procedure as well.

4.7.4 Acceptance of renewed certificates

Renewed certificates are accepted according to the rules in Section 4.4.

4.8 Certificate revocation

4.8.1 Reasons for certificate revocation

A certificate is revoked:

- on its expiry date when no application for renewal is submitted by the Owner;
- in case of termination of the legal person of the CSProvider with no transfer to another certification services provider.

The CSProvider is obliged to revoke the certificate upon request by the Owner/Signatory after checking the identity and representative powers of the Owner or Signatory, respectively.

The CSProvider revokes the certificate in case of:

- death or legal prohibition of the Owner/Signatory;
- termination of the legal person of the Owner;
- termination of representative powers of the Signatory regarding the Owner;
- establishing that the certificate was issued on the bases of incorrect data.

4.8.2 Who can apply for certificate revocation

Only the Owner or a duly authorized by him person can submit an application for certificate revocation.

4.8.3 Order for submission of application for revocation of certificates

The order for submission of applications for revocation of a certificate issued by the CSProvider is described in the issuance and management policy for the particular type of certificate which is part of the *Certificate Policy*.

4.8.4 Checks in the certificate revocation list

The CSProvider supports an updated at every three hours public list of revoked certificates (CRL) for status checks. For this purpose the CSProvider publishes the data from the certificates and CRL (Certificate Revocation List) in an own, accessible for everyone electronic archive. This archive can be accessed via LDAP protocol (Lightweight Directory Application Protocol)

Each user and/or relying party has to check the status of the certificate in the Certificate revocation List every time when he has to decide whether to trust the information from a particular certificate. The CSProvider is not responsible for any damages to the relying parties when no status checks on the certificates are made.

The Certificate Revocation List is available 24 hours on the following address:
<http://www.spektar.org> .

4.8.5 Online status checks (OSCP)

The CSProvider offers the possibility to check the status of the issued certificates in real time using the necessary equipment and technologies. This service allows the Relying parties to receive information on the status of the certificate at the current moment.

To make online checks on data from the register one needs suitable software (OSCP client or access via the website of the certification services provider: <http://www.spektar.org>).

5. Management, procedural and physical security measures

5.1. Physical security measures

Security measures regarding physical security are an element of the developed and implemented CSProvider information security system in accordance with the requirements of the ISO 17799 standard.

Measures regarding physical security of data, systems, premises and connected to them supporting systems aim to prevent from:

- unauthorized access, harm and intervention in work conditions;
- loss, harm or discredit of resources;
- discredit or theft of information or means for data processing.

5.1.1 Layout and structure of operating teams

The Certification Authority and Registration Authority of the CSProvider work in structures corresponding to the requirements of the management of the CSProvider for security and audit. These structures are protected regarding discovery and prevention of obvious or obscure security breaches.

5.1.2 Premises

The CSProvider has specially equipped premises with highest level of protection regarding physical access, in which all central components of the PKI-infrastructure are kept.

These premises are not used together with other departments and organizations of Spektar AD.

5.1.3 Physical access

The CSProvider's systems have several levels of physical security, demanding initial access to a lower level before obtaining access to a higher level. There are progressively restricting access rights for every level. The key activity of the Certification Authority is carried out at the highest protection level. All actions of the employees are recorded. Unaccompanied visitors are not allowed to the high security levels. The physical security system requires additional security levels for operations for key management. Access to them is restricted in accordance to the CSProvider's policy for position division. Visits to these levels are recorded.

Physical access to premises under 5.1.3 is controlled by access control systems, video surveillance, signal-notifying systems, etc.

The physical access control systems are inspected regularly and journals are kept.

Authorized employees of the CSPProvider observe and follow internal procedures for access to different zones of the premises with restricted physical access.

Each employee of the CSPProvider is personalized in the systems which control the access to the premises and there is strict verification needed in order to obtain access.

5.1.4 Power supply and ventilation

The CSPProvider's structures are equipped with main and duplicate power supply systems supplying power continuously, which are protected from external interventions.

Power supply for all central components of the CSPProvider's structure is protected from central blackouts.

The ventilation system is specially designed for such premises and does not allow discredit of the physical and electromagnetic security of the premises and guarantees normal functioning of the installed computer components.

5.1.5 Measures against flood

The CSPProvider takes the necessary measures to reduce the risk of flood.

5.1.6 Anti-fire precautions

The CSPProvider takes all necessary measures to prevent and minimize the risk of fire. These measures are designed to comply with the operating legal and standardization acts regulating anti-fire protection.

5.1.7 Duplicates of crucial information

All carriers of software, archives of data or audit information are kept in the structures of the CSPProvider or in a secured zone with suitable system for physical and logical security, restricting access and protecting carriers from possible harm (exposition to electromagnetic harm or other).

Copies of information regarded as crucial and confidential (journal information for system work, activating data for cryptographic devices/modules, system archive information (back-up), etc.) are kept in special premises. In some cases, defined with the internal rules for information keeping the information can be kept in specialized premises outside the CSPProvider's building.

5.2 Procedural security measures

5.2.1 General organization rules

All procedures regarding security of issuance, administration and application of the certificates for electronic signature are carried out by employees of the CSProvider.

The CSProvider maintains sufficient number of qualified employees who can always act in accordance with the operating legislation and organization's internal rules and regulations.

5.2.2 Function distribution

There is a detailed distribution of functions and responsibilities of the personnel in the organization's documents (job descriptions, pay-roll schedule) and respective internal operating procedures.

The distribution of functions is designed to minimize the risk of discredit, leak of confidential information or personal data and conflict of interests.

5.3 Security measures regarding personnel

5.3.1 Personnel qualification

The personnel is recruited in accordance with the internal documents and pay-roll schedule of the CSProvider and complying with the requirements for the respective job position regarding theoretical and practical skills and qualifications, personal records, etc.

People wishing to take a particular job position present proofs for their experience and qualification necessary for the execution of their work responsibilities.

The CSProvider uses methods for personnel research within the legal framework. Use of the collected information is in accordance to the operating legislation.

5.3.2 Personnel training

The CSProvider trains its personnel for the successful fulfillment of their work responsibilities related to:

- PKI-technology;
- Functions, duties and responsibilities related to specific operations and processes;
- Policies and procedures of the CSProvider;
- Application of software and hardware;
- Crisis handling;

- Recovery and maintenance of normal work process.

5.3.3 Sanctions for breach of security rules

In cases when an employee breaches the rules and regulations stipulated in the policies, security procedures and other internal documents the necessary disciplinary and administrative measures are taken depending on the disciplinary/administrative breach of the operating legislation.

5.3.4 Outsourcing

In rare cases independent contract persons or consultants can take the positions of trusted persons (personnel) in accordance with the procedures of the organization.

5.3.5 Documentation presented to personnel

The CSPProvider gives to its employees the documentation they need to perform their duties and functions for the job position they have.

5.4 Security check procedures

5.4.1 Types of recorded events

The CSPProvider record manually or automatically the following events:

- events regarding validity period of the Certification Authorities keys, which include:
 - key generation, keeping, recovery, archiving and destroying;
 - events from the validity period of the cryptographic devices.
- events from the validity period of the certificates of Certification Authorities and end users:
 - applications for certificates, renewal, recoding, suspension and revocation;
 - successful or unsuccessful processing of the applications;
 - creation and issuance of certificates and lists for suspended and revoked certificates.
- events related to security including:
 - successful and unsuccessful attempts for access to the system of the managed public keys infrastructure;

actions by the CSPProvider's employees related to the security of the managed public keys infrastructure;
significant for security files or records, read, written or deleted;
changes in the security profile;
cracks in the system, hardware flaws and other anomalies;
visitors in the sites of the Certification Authorities.

The records kept have the following elements:

- date and time of input;
- serial or consecutive number of input for automated journals;
- identity of the authority recording the event;
- type of record.

The Certification Authorities of the CSPProvider and PKI administrators keep reports of the information from the applications for certificates including:

- type of the identity document(s) presented by the applicant;
- unique identification data or identity documents;
- location of the copies of application forms and identity documents;
- identity of the authority accepted the application;
- method of validation of the identity documents.

5.4.2 Frequency of recording

Security assessment reports are reviewed at least once weekly for significant events regarding security. Additionally the CSPProvider reviews its reports for unusual activity in response to sent warnings, based on irregularities or incidents with the registration and certification authorities of the CSPProvider.

Security assessment reports consist of reviews of the reports and documentation for all significant events. In the security assessment reports there is a certification that the report is not forged by the revision of all data in the report and investigation into all irregularities in the reports. All actions related to this are also documented.

5.4.3 Keeping period of the reports

The reports are kept for at least two months after their processing and after that are archived in accordance with Section 5.5.2.

5.4.4 Report protection

Reports are protected from unauthorized reviews, modifications, deletion or forgery by use of physical and logical access control.

5.4.5 Procedures for keeping reports

Partial copies of the reports are created daily and full copies are created weekly.

5.4.6 System for keeping data from security assessments

Automated information is created and recorded at levels application, network and operating system. Manually processed information is recorded by CSPProvider's employees.

5.4.7 Notification of persons causing the events

Notification of collection of data and event registration is not sent to the person or device causing the event.

5.4.8 Vulnerability assessment

Assessments of the vulnerability of the logical security are carried out and reviewed after research of the observed events. Assessments of the vulnerability of the logical security are based on automatically generated information recorded in real time and are carried out daily, monthly and annually in accordance to the requirements of the management for security and assessment. The annual assessment of the vulnerability of the logical security is included in the annual assessment of compatibility.

5.5 Archiving records of CSPProvider's activities

5.5.1 Types of events recorded

In addition to the security assessment reports regulated in Section 5.4 the CSPProvider keeps records which include documentation on:

- compatibility of the CSPProvider with the certificate policy and other liabilities implemented in agreements with end users;
- action and information of crucial importance for each application for certificate and creation, issuance, use, suspension, revocation, renewal and expiry of all certificates issued by the Certification Authority of the CSPProvider.

Records of the CSPProvider for the validity period of certificates contain:

- identity of the end user of each certificate;
- identity of the persons applied for suspension or revocation of the certificate;
- other facts from the certificate, time logs;
- some foreseeable facts related to the issuance of the certificate including but not limited to information on successful compatibility assessment in accordance with Section 2.5.

Records can be kept in electronic form or on a hard carrier in regard with precise and full indexing, keeping and reproduction.

5.5.2 Keeping period of the archives

Records related to certificates are kept until the CSPProvider functions as a certification services provider.

If necessary the CSPProvider can keep records for a longer period of time in regard with observing the operating legislation.

5.5.3 Archive protection

The CSPProvider keeps the archived records so that only authorized and trusted persons have access to them. Information is archived electronically and is protected from unauthorized viewing, modification, deletion or forgery through the implementation of a suitable logical and physical access control. The carrier on which the recorded information is kept and applications for its processing are maintained aiming to provide access to this information for the period of time stipulated in Section 5.5.2.

5.5.4 Procedures for archive keeping

The CSPProvider makes copies of its electronic archives containing information on issued certificates daily and full copies weekly. Paper copies of the information is kept are kept in a structure protected from disasters in accordance with Section 5.6 (recovery from crisis).

5.6 Actions in cases of disaster, failure or compromise of the keys of the CSProvider

The CSProvider has implemented a stable combination of physical, logical and procedural means of control aiming to minimize the risk of crisis or key disclosure. There are additional procedures for recovery after crisis which are described in Section 5.6.2 and procedures following key disclosure, described in Section 5.6.3. These procedures have been created to minimize the impact of such events and easier recovery to the normal functioning of the CSProvider for a reasonable period of time regarding trading relations with clients.

5.6.1 Damage to computer resources, software and/or information

In cases of damaged computer resources, software and/or information the crisis handling procedures of the CSProvider are initiated. These procedures require adequate and quick reaction, investigation of the incident and actions to recover from the damages. If necessary the procedures of the CSProvider for recovery from crisis are initiated.

5.6.2 Recovery from crises

The CSProvider has created, implemented and tested a plan for recovery from crises to limit the effect of forces of nature or disasters. This plan is tested and reviewed regularly in order to be optimized.

The detailed plans for recovery from crises aim to restore the information systems and basic business functions. There are implemented systems for physical protection and control on the activities which meet the requirements in the manual on security and security assessment in order to provide stability in business for the CSProvider.

In cases of natural crisis or crisis caused by humans which results in permanent or temporary interruption of the business of the CSProvider a special emergency team is initiated.

The CSProvider has the opportunity to restart its activities within twenty-four (24) hours after the crisis with minimal support of the following functions:

- certificate issuance;
- certificate suspension;
- publishing information on suspended certificates.

The database of the CSProvider for recovery from crises is regularly synchronized with the products database within certain deadlines stipulated in the manual on requirements for security and

audit. The equipment of the CSPProvider for recovery from crises is protected by systems for physical security comparable with those in Section 5.1.1.

The CSPProvider's plan for recovery from crises is created to ensure full recovery of all functions of the CSPProvider within a week after a crisis affecting the main structures. The CSPProvider tests its equipment in the structure in order to maintain the functions of Certification and Registration authorities after a big crisis which would stop the functioning of the whole structure. The results from these checks are used for assessment and planning purposes. When possible the activities of the CSPProvider's structure are recovered as soon as possible after a major crisis. Private keys of the Certification authorities are archived and kept for the purposes of the recovery from crises process in accordance with Section 6.2 (Key protection).

Copies of important information are kept by the certification authority of the CSPProvider. This information includes but is not limited to: information on applications for certificates, information on security assessments according to Section 5.4 (Security procedures) and a database of all issued certificates.

5.6.3 Disclosure of keys

In cases of suspected or established disclosure of keys of a Certification authority of the CSPProvider the procedures for reaction to key disclosure of the CSPProvider are initiated. These procedures are led by experts and representatives of the CSPProvider. Their task is to analyze the situation, to create an action plan and take measures for recovery approved by the management of Spektar AD.

The following procedures are followed if suspension of the certificate of the certification authority is needed:

- information on the status of the suspended certificate is sent to all persons under the rules of Section 2.7;
- reasonable efforts are made to inform all concerned participants in the secure network of the CSPProvider;
- generation of a new key pair of the certification authority in accordance with Section 5.7 (Change of the keys of a Certification authority) except in cases of termination of the activities of the certification authorities according to Section 2.7 (Termination of the activities of the Certification services provider).

5.7 Change of the keys of a Certification authority

The private-public key pair of a Certification authority can be renewed in the following cases:

- expired validity of the private-public key pair;
- introduction of new services by the CSPProvider which require changed parameters of the private-public key pair (an increased length of the key, for example).

The change of the private-public key pair of a Certification authority of the CSPProvider shall observe the following rules:

- The Certification authority whose private-public key pair will be changed stops issuing certificates for subordinate Certification authorities (if there are any) 60 /sixty/ days before the moment when the rest of the validity period of its key pair equals the validity period of the certificates issued by its subordinate Certificate authorities;
- The Certification authority whose key pair is changed continues to publish a certificate revocation list which is signed with the old key pair until the expiry date of the last certificate issued:
 - with the old private-public key pair of the Certification authority;
 - by a subordinate Certification authority whose certificate is signed with the old private-public key pair.

6. Technical security measures

This part describes the procedures for generation and management of the private-public key-pairs for:

- Certification Authorities of the CSPProvider;
- Registration Authority of the CSPProvider;
- end users.

The CSPProvider generates the private-public key pair of the Certification Authorities and Registration Authority using a secure mechanism for the creation of a signature with protected profile, determined in accordance with the security levels specifications.

In cases when the private-public key pair is generated by the Owner/Signatory he is fully responsible for the protection of the private key in order to prevent its discredit, disclosure, modification, loss or unauthorized use. The Owner/Signatory is responsible for omissions or actions of

persons authorized by them to generate or keep their private keys.

6.1 Generation of the private-public key pair

6.1.1 Generation of the private-public key pair of the Certification Authority Spektar Root CA

A member of the Board of Directors of Spektar AD, the Manager of *Certification Services Team*, the Security Manager, a notary public and other authorized persons attend the procedure for generation.

The installed crypto-module (HSM) has the highest security level in accordance with the requirements of the international standards and those of Bulgarian legislation (FIPS 140-2 Level 3).

Only the Manager of the Certification Services Team and the Security Administrator run the procedure for access to the module and generate the basic key pair.

The Manager of the CST and the Security Administrator independently generate symmetric keys (Triple DES keys) which are kept on smart cards protected with access passwords (Pass phrase).

- each operating card contains only a part of the generated keys;
- operating cards protect the keys kept in the module;
- both operating smart cards and respective pass phrases are needed to manage the keys kept in the module.

The generation of the basic key pair is initiated according to the profile of the basic *Spektar Root CA certificate* (RSA, 4096 bits).

- the Manager of the CST and the Security Administrator independently confirm the generation of the key pair with operating smart card and pass phrase;
- the extraction of the generated private key from the crypto-module is impossible;
- use of the private key is only possible in the presence of the two operating smart cards and respective pass phrases.

Only persons authorized according to the *Security Policy* have physical access to the workplace of the provider after initiation of the basic key pair.

The crypto-module is deactivated after successful generation and initiation of the basic key pair.

The pass phrases of the operating smart cards are changed and kept until the next use of the crypto-module.

The operating cards are kept in self-contained and independent cassettes in a safe with the highest level of physical protection.

6.1.2 Generation of the private-public key pairs of the Certification Authorities Spektar Universal CA and Spektar NonUniversal CA

The key pairs of the other components of PKI (SpektarUniversal CA, Spektar NonUniversalCA) of the CSPProvider are generated by the Security Administrator. An HSM module which is certified for security level corresponding to FIPS 140-1 Level 3 is used.

The Security Administrator generates the key pair as follows:

- the key pair of Spektar Universal CA for signing certificates of the Spektar Universal Certificate type;
- the key pair of Spektar NonUniversal CA for signing certificates of the Spektar NonUniversal Certificate type.

Smart cards with level of security corresponding to FIPS 140-1 Level 1 are used for the generation of the key pair of Spektar RA(Enroll) for certification of electronic application and internal certificates in the structure of the provider. The key pair remains in the smart card which provides high security level and reliable keeping.

After the generation of the key pair physical access to the work premises of the provider is permitted only for the persons authorized for this according to *Security policy*.

6.1.3 Generating a private-public key pair for users' certificates

6.1.3.1 Distant generation of a key pair by the Owner/Signatory

The Signatory loads his personal form for generation of a key pair on the system of the provider.

The specially developed for this purpose software of the provider together with the respective CSP for management of the user's reader and smart card run the process of generation of a key pair.

The saving and keeping of the private key is at high security level which is guaranteed by the carrier itself (smart card), secured by PIN which is known only to the Owner or Signatory (duly authorized according to the respective form-example).

The Signatory generates the electronic application in PKCS#10 format and sends it to the CSPProvider. According to recommendations RFC 2314 the PKCS#10 format contains DN, the public key and other attributes, all signed with the private key and packed in ASN.1 format.

6.1.3.2 Generation of key pairs in the CSPProvider

The Signatory in the presence of a duly authorized officer of the Registration Authority of the CSPProvider loads his personal form for generation of a key pair on the system of the provider.

The specially developed for this purpose software of the provider together with the respective CSP for management of the user's reader and smart card run the process of generation of a key pair.

After the key pair is generated the Signatory himself changes the PIN code for access to the smart card.

The saving and keeping of the private key is at high security level which is guaranteed by the carrier itself (smart card), secured by PIN which is known only to the Owner or Signatory (duly authorized according to the respective form-example).

A duly authorized person from the structure of the Registration Authority of the CSPProvider generates the electronic application in PKCS#10 format before the Signatory.

6.1.4 Submission of private keys

The private-public key pair is generated and kept by the Owner/Signatory.

6.1.5 Providing public keys by the Owner/Signatory to the CSPProvider

This procedure is only run by the Owner/Signatory.

The Owner/Signatory sends an electronic application in PKCS#10 format. The application contains the public key of the Owner/Signatory and is signed electronically with the corresponding private key.

By checking the authenticity of the signature the CSPProvider can establish the authenticity of the sent key as well.

6.1.6 Providing public keys to the Certification Authorities of interested persons

The public keys of the provider (Basic – Spektar Root CA and operating – Spektar Universal CA and Spektar NonUniversal CA) are publicly accessible on the website of the CSPProvider: <http://www.spektar.org/>.

The CSPProvider assures access to Spektar Root CA, Spektar Universal and Spektar NonUniversal CA operating certificates in the public registry for at least 2 (two) years after the validity of these certificates expires.

6.1.7 Key length

The length of the basic key (of Spektar Root CA) is 4096 bites.

The length of the operating keys of the Certification Authorities of the CSPProvider (of Spektar Universal CA and Spektar NonUniversal CA) is 2048 bites.

The minimal recommended length of a key of an Owner/Signatory is 1024 bites (RSA).

6.1.8 Application of keys (according to KeyUsage field)

The used X.509 v.3 format of the certificates for universal signature allows defining of extensions and/or restrictions in accordance with the particular profile of the certificate, typical for the specific usage.

There is a description of the extensions used in Section 7 of this document.

6.2 Protection of private keys

6.2.1 Standard for cryptographic modules

The private keys corresponding to the Basic (Spektar Root CA) and Operating certificates (Spektar Universal CA, Spektar NonUniversal CA) of the CSPProvider are kept in secure cryptographic modules which meet the normative requirements.

The installed crypto-modules are with the highest level of security according to the requirements of the international standards and those stipulated in the Bulgarian legislation (FIPS 140-2 Level 3).

The smart cards used have security level corresponding to FIPS 140-1 Level 1.

6.2.2 Keeping and control of private keys

6.2.2.1 CSPProvider's keys

The basic key of the CSPProvider is enciphered by a symmetric key divided into several separate and independent parts and is constantly kept on the crypto-module.

The functions creation, keeping and usage of the private key of the certification services provider are delegated in a written form to the Board of Managers of Spektar AD.

The procedure for keeping the private key according to Section 6.11 is run simultaneously with the generation of a key pair of the Certification Authority.

6.2.2.2 Users' keys

Only the Signatory has right of access to the private key corresponding to the public key in the issued certificate. The CSPProvider offers the service of generation of a private-public key pair when the keys are generated on a smart card without possibility of extraction of the private key. The smart card is given to the Signatory.

6.2.3 Input of keys in crypto-modules

Symmetric keys are input in crypto-modules of the systems according to the regulations of Section 6.1.1 by the authorized persons who shall enter the separate parts of this key independently form each other.

6.2.4 Methods for deactivation of private keys

6.2.4.1 Activation of a symmetric key in HSM

The symmetric key for encipherment of the basic key of the CSPProvider is activated in HSM by system administration passwords entered by the Security Administrator and the Manager of the CST.

6.2.4.2 Activation of private keys in smart card

The private key of the Owner can be accessed by putting the smart card into the reader and entering the PIN.

6.2.5 Methods for deactivation of private keys

6.2.5.1 Deactivation of a symmetric key in HSM

The symmetric key for encipherment of the basic key is deactivated by pulling out the cards of the Security Administrator and Manager of the CST from the HSM.

6.2.5.2 Deactivation of private keys

Private keys are deactivated by revocation of the certificate by which the generated key pair is certified and the public part of which is included in the issued certificate.

To terminate the use of a private key from a smart card the smart card is pulled out of the reader and control of access to the smart card realized through the PIN is stopped.

6.2.6 Method for destruction of private keys

The private key of the Certification Authority is destroyed through initialization of the crypto-module and destruction of the parts of this key kept in the archive.

The destruction of the private key is done through:

- initialization (“erasure”) of the smart card;
- physical destruction of the carrier.

6.3 Additional aspects of key management

6.3.1 Public keys archive

The public keys are kept in a database of the CSPProvider and are archived periodically for a time corresponding to the validity period of the operating certificate of the Certification Authority.

Certificates which contain the public keys of the Owners are kept in the Electronic registry of the CSPProvider.

6.3.2 Validity period of certificates

The certificates have the following validity periods:

- basic certificate (Spektar Root CA) – 20 years;
- operating certificate (Spektar Universal/NonUniversal CA) – 5 years;
- Owner's certificate – 1 year.

The use of a key with expired validity of the certificate is not valid and the signed object or statement shall be considered not signed.

The public keys for checks of validity of the electronic signature are always available as part of the published certificates in the Public Registry of the CSPProvider.

6.4 Means for activation of private keys

The Signatory is obliged to keep from compromise the personal data for activation of his smart card or key file (his PIN or password).

6.5 Computer system protection

The CSPProvider has developed and follows policies, procedures and methods for administration and management of the security of the infrastructure used in accordance with the general international standards for management of the information security.

Security measures taken regarding the computer systems are an element of the developed and implemented CSPProvider's system for information security and aim to reduce the identification and assessment risks to a reasonable level.

The security measures regarding the computer systems aim to protect, stop, discover, react and recover and can be used for several of the mentioned functions simultaneously.

The reliability of the systems used as well as the technical and cryptographic security of the processes run by them are provided by running tests and checks of the computer information systems.

6.6 Development and exploitation

Equipment in the CSPProvider is divided into operating, developing and testing. The development of products related to the certification services offered by the CSPProvider is done by separate systems,

completely independent from those in operation.

All products, software and services offered by the CSPProvider are tested initially in the systems for development and testing before they are implemented and offered to the users.

The services offered by the CSPProvider are supported by fully self-contained and specially designed computer information systems.

6.7 Network security

The CSPProvider has certain practices, measures and principles regarding network security, control and giving rights to network information resources. The CSPProvider uses state-of-the-art network technological means (hardware and software) to protect access and information exchange within its structure through the following:

- restricting physical access to active equipment and cables;
- physical separation of the network;
- using network protocols which allow restrictions for the users;
- logical separation of the networks (VLAN);
- restricting access to network resources at application level for users;
- restricting access to/from external networks;
- protected communications – SSL/TSL communication.

7. Profile of issued certificates and of the certificate revocation list (CRL)

7.1 Profile of issued certificates

Certificates issued by the CSPProvider are in accordance with:

- ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework;
- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Issued certificates always contain the basic fields described in the table below:

Serial Number	Serial number of the certificate
Signature Algorithm	Algorithm used by the Certification Services Provider for signing the certificate
Issuer DN	Name of the Certification Services Provider issued the certificate

Valid From	Date from which the certificate is valid
Valid To	Date to which the certificate is valid
Subject DN	Name of the Owner/Signatory. In accordance with the profile of the particular certificate from the <i>Certificate Policy</i>
Subject Public Key	Public Key of the Owner/Signatory
Signature	Signature of the Certification Authority generated and enciphered in accordance with RFC 3280.

The precise content of the profile of each particular certificate is given in the policy in accordance to which it has been issued.

7.1.1 Version of issued certificates

The certificates issued by the CSPProvider are X.5009 Version 3.

7.1.2 Extensions of issued certificates

The X.509 Version 3 format used by the CSPProvider for the certificates issued allows defining of extensions and/or restrictions in the application of the certificate in accordance to the respective profile. Fields which define these extensions and/or restrictions:

7.1.2.1 Key usage – defines use of the key which is in the certificate issued and the respective restrictions for legal value of the signature of the used certificate. According to recommendations X.509 v.3 the following uses of certificates are possible:

- Digital Signature – for checks of electronic signatures which help identify users or integrity of data;
- NonRepudiation – to prove the fact of the statement. When data is electronically signed the electronic signature proves that it is authentic and intact;
- Key encipherment – for encipherment of keys as well as for exchange of keys through unsecured transfer environment;
- Data encipherment – for encipherment of data which is archived or transferred;
- Key Certificate Signing – used only in certificates of the Certification Authorities, for checks of electronic signature of a Certification Authority;
- CRL Signing - used only in certificates of the Certification Authorities, for checks of the electronic signature of a Certification Authority with which the supported by it CRL is signed.

7.1.2.2 *Certificate policy* – shows the policy which the certification services provider has followed to issue the certificate in accordance to its particular use.

7.1.2.3 *Basic Constraints* – defines the type of the Owner and Signatory (Subject) – is the issued certificate one of the certification authority or a certificate of an end user. The *Basic Constraints* field is crucial.

7.1.2.4 *Enhanced Key Usage* – shows the application, issuance policy and type of the certificate.

7.1.3 Algorithm for signing certificates issued by the CSPProvider

The CSPProvider uses the Sha1RSA algorithm for signing the certificates it issues by applying:

- Hash-function – Sha1(Secure Hash Algorithm);
- Algorithm for encipherment – RSA(Rivest-Shamir-Adelman).

All certificates issued by the CSPProvider and signed with Sha1RSA algorithm comply with the requirements of recommendations RFC3279.

Information for the algorithm used for signing the certificate can be found in the *Signature Algorithm* field of its profile.

7.1.4 Form and restrictions for names used

Names in the fields of the certificate shall be written in accordance with the requirements and restrictions of the recommendations of X.501.

The rules for use of names and conflict solving described in Section 3.1 shall be applied.

7.1.5 Identification of the policies for certificate issuance

Each of the policies according to which certificates are issued by the CSPProvider is given an object identifier (OID). The object identifier is a unique line of whole numbers.

A list with identifiers of the policies for certificates issued by the CSPProvider is given in *Certificate Policy* (Section 2).

7.2 Profile of the Certificate revocation list (CRL)

The certificate revocation list published by the CSPProvider complies with the requirements of the

RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) and contains the following fields:

Version	Version of the certificate revocation list according to 7.2.1 of this document
Issuer	E ca@spektar.org
	Phone +359 2 9699 200
	CN Name of the certification authority published this list
	OU Spektar CA
	O Spektar JSC, B: 831431323
	L Sofia
	S Sofia
C BG	
Effective date	Date of publication of the list in format: [dd Month gggg hh:mm:ss]
Next update	Date of publication of the next update of the list [dd Month gggg hh:mm:ss]
Signature algorithm	Sha1RSA – algorithm used for signing the list by the Certification authority according to the international specification RFC 3279 (Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)
Authority Key Identifier	KeyID=[XXX...] – identifier of the Certification Authority
CA Version	VX.X
CRL Number	[XXX...]
Next CRL Publish	Day, Month, dd, gggg hh:mm:ss
Published CRL Locations	[1]Locations Distribution Point Name: Full Name: URL=ldap:///CN=Spektar Universal CA, CN=universal,CN=CDP, CN=Public Key Services, CN=Services,CN=Configuration,DC=spektar, DC=org?certificateRevocationList?base?objectClass=cRLDistributionPoint
Revocation List	List of suspended and revoked certificates which contains the following information for each certificate in the list: certificate serial number; date of suspension or revocation.

7.2.1 Profile version

The Certificate Revocation List (CRL) published in the electronic registry on the CSPProvider is Version 2.

7.2.2 Codes for suspension and revocation of certificates

The code shows the reason why a particular certificate is in the Certification Revocation List (CRL) of the CSPProvider and it can have one of the following values:

- *Key Compromised* – discredited private key of the Signatory;
- *CA Compromised* – discredited private key of the Certification Authority with which the users' certificates are signed;
- *Affiliation Changed* – changed relations between Signatory and Owner – change in the company, change of the representative authority, deprivation of representative powers,

termination of work relations, etc.;

- *Superseded* – certificate is changed with another certificate;
- *Certificate Hold* – certificate is suspended.

8. Other business and legal provisions

8.1 Financial conditions

The CSProvider offers certification and other services for payment.

Payment for certification and other services which will be provided to the Owner is determined in accordance with *Certification Services Application*, an integral part of the certification services contract, observing the prices published in the *Price List*. The Price List published on the CSProvider's website contains updated information on prices for the services offered.

The CSProvider retains the right to unilaterally change the announced prices and timely inform the CRC for any changes. Price changes do not affect paid fees.

The CSProvider sets prices for the following services:

Certificate issuance

- certificate renewal;
- certificate renewal after changes in the public part by the Owner/Signatory;
- technological help and consultancy.

The CSProvider offers the following services for free:

- TimeStamp access;
- Access to the CRL;
- OSCP access.

There is one-time payment of the fee for certification services and should be done before certificate issuance.

Payment for technological help and consultancy is one-time after the technological help and consultancy and after their duration is established.

Payment can be made by bank transfer to a bank account given by the CSProvider or in cash in the

office of the CSProvider.

For payment by bank transfer payment date is considered the date of verification of the CSProvider's account.

8.2 Insurance policy

8.2.1 Compulsory insurance

The CSProvider is insured for the time it acts as a certification services provider against possible harms due to failure to fulfill its duties under the EDESA.

8.2.2 Insurance coverage

The compulsory insurance covers the liability of the CSProvider for all non-material and substantive damages to the Owner of the universal electronic signature and to all third parties under article 29 of the EDESA; the insurance amount is as stated in the ORDINANCE on the Activities of Certification-Service-Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services.

8.3 Applicable legislation. Conflict solving and jurisdiction

For all matters not regulated in this document the operating legislation in Bulgaria shall be applied.

All conflicts regarding certification services provision shall be solved by negotiations.

Claims related to the activities of the CSProvider can be submitted:

- electronically to: delovodstvo@spektar.org;
- in the records office of the *Registration Authority* of Spektar AD, Sofia, 11A Carnegie street.

Claims are considered within two weeks of receipt. The Manager of the *Certification Services Team* gives a reply stating reasons of which the claimer is informed by a CSProvider's officer in a way prearranged by the claimer.

In case voluntary regulation of the relations is not possible, the matter shall be taken to the court of competence.

For substantive conflicts arisen after the signing of the certification services contract the court of

competence is the respective regarding rank court in Sofia in accordance with article 91 of the Code of Civil Procedure (CCP).

8.4 Management of the *User's Manual* document

The *User's Manual* consists of the following documents:

- *Certificate Practice Statement;*
- *Certificate Policy.*

8.4.1 *User's Manual* distribution

The updated version of the *User's Manual* is published in the electronic registry of the CSPProvider.

According to the rules in Section 2.4 there are no restrictions for access to the documents.

8.4.2 Updates of the *User's Manual*

Changes in the *User's Manual* can be made only by authorized officers of the CSPProvider upon suggestion by:

- state bodies controlling the activities of the CSPProvider;
- management of the CSPProvider;
- auditors carrying out internal audits of the information security system.

All changes in the *User's Manual* shall be approved of the Communications Regulation Commission before their enactment.

9. Glossary

A	Actuality
Advanced electronic signature	Advanced electronic signature is a transformed electronic statement included, added or logically connected to the same electronic statement before transformation
ASN.1	Abstract Syntax Notation One
BG	Bulgaria
C	Country
CA	Certification Authority, CA Sektor CA is a separate subgroup of the Certification Services Team in the structure of Spektar AD, which runs the activities for certification services provision. The Certification Authority is not an independent legal entity and all actions by its employees are in their capacity of employees of the CSPProvider, within their powers
CC	Common Criteria
CD	Compact Disk
Certification	Certification Services Provider(CSPProvider) <i>Spektar AD</i> acting as a provider of

Services Provider	certification services through physical persons and the functionally created organization structure <i>Certification Services Team</i>
Certificate for advanced electronic signature Certificate	The certificate for advanced electronic signature is an electronic document, signed by the CSPProvider, containing certain properties and certifying the connection between the Owner/Signatory and his public key for checking signed documents and objects and giving a possibility to establish the identity of the Owner and this of the Signatory
Certificate for universal electronic signature	Certificate for universal electronic signature is issued by a registered CSPProvider. The Certificate is of the Spektar Universal type and contains the stipulated in article 24 of the EDESA properties
CN	Common Name
CRL	Certificate Revocation List
CP	The Certificate policy is a document, integral part of the User's manual, describing the policy the provider follows for issuance of certificates, as well as for all other services
CPS	The Certification Practice Statement is a document – integral part of the User's manual, containing rules for issuance, suspension, renewal and revocation of certificates; conditions for giving access to certificates, as well as security measures
CRC	Communications Regulation Commission
CS	Certification Services
CSP	Cryptograph Services Provider
CST	Certification Services Team
DN	Distinguished Name
DSA	Digital Signature Algorithm
E	E-mail
EGN(PIN)	EGN (Personal identification number)
EDESA	Electronic Document and Electronic Signature Act
Electronic Signature	Any piece of information related to the electronic statement in a way coordinated between the Signatory and the addressee, safe enough regarding the circulation needs. The electronic signature reveals the identity of the Signatory and his consent with the electronic statement and protects the content of the electronic statement from consequent changes. The signing is done by using a key pair and algorithms for asymmetric cryptography
Enhanced key usage	This field indicates the enhanced key usage
FIPS	Federal Information Processing Standard
HSM	Hardware Security Modul
IP	Internet Protocol
ISO	International Standardization organization
JSC	Joint Stock Company
L	Location
LDAP	Lightweight Directory Access Protocol
Manual	User's manual for the offered by Spektar AD certification, informational, cryptographic and consultancy services. The manual has the effect of general provisions and consists of the following documents: 1. Certification Practice Statement, CPS 2. Certificate Policy, CP
N	Number
O	Object
OACSP	Ordinance on the Activities of Certification-Service-Providers,

	the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services (Promulgated, SG No. 15 dated 8 February 2002, in effect from 12.02.2002)
OCSP	On-line Certificate Status Protocol
OID	Object Identifie
OPRCSP	Ordinance on the Procedure for Registration of Certification-Service-Providers (Promulgated, SG No. 15 dated 8 February 2002, in effect from 12.02.2002)
ORAAES	Ordinance on the Requirements to the Algorithms of Advanced Electronic Signature (Promulgated, SG No. 15 dated 8 February 2002, in effect form 12.02.2002)
OU	Organization unit
Owner	The Owner is a physical or legal person on behalf of whom signed electronic statements are created and stated in the issued certificate as Owner
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PIN	Personal Identification number
PSE	Personal Security Environment
Relying Parties	The Relying Parties are physical or legal persons – addressees of electronic statements signed with electronic signatures for which there are certificates for electronic signature issued by a CSPProvider or of processed electronic information or data, through PKI technologies, based on the services offered by the CSPProvider - certification, other informational or cryptographic
RP	Responsible Person
RSA	Rivest-Shamir-Adelman cryptographic algorithm
S	Street
SHA	Secure Hash Algorithm
Signatory	The Signatory is a physical person who creates electronic statements on behalf of the Owner and signs them in accordance to the representative powers given to him and who is stated as a Signatory in the issued certificate
SMIME	Secure Multipurpose Internet Mail Extensions
SSCD	Secure Signature Creation Device
SSL	Secure Socket Layer
T	Title
Universal electronic signature	Universal electronic signature is the advanced electronic signature for which the certificate is issued by the certification services provider, registered under article 34 of the EDESA
URL	Uniform Resource Locator