



# CERTIFICATE POLICY

**Revision: 3.1**

**Spektar AD**  
**11A Carnegie street**  
**1000 Sofia, Bulgaria**  
**phone: + 359 2 9699 200**  
**fax: + 359 2 9699 255**  
<http://www.spektar.org>

**CONTENT**

1. Introduction .....	5
2. Services offered.....	5
2.1 Certificate issuance and management.....	5
<a href="#">2.1.1 Issued user's certificates.....</a>	<a href="#">6</a>
<a href="#">2.1.2 Basic certificate of the CSProvider.....</a>	<a href="#">7</a>
<a href="#">2.1.3 Operating certificate for universal electronic signature of the CSProvider Spektar Universal CA.....</a>	<a href="#">8</a>
<a href="#">2.1.4 Identification of the policies for issuance and management of certificates for universal electronic signature.....</a>	<a href="#">10</a>
<a href="#">2.1.5 Operating certificate for advanced electronic signature Spektar NonUniversal CA.....</a>	<a href="#">10</a>
<a href="#">2.1.6 Identification of the policies for issuance of certificates for advanced electronic signature.....</a>	<a href="#">11</a>
2.2 Maintenance of an electronic public registry.....	12
2.3 Access to the Certification Revocation List (CRL) via HTTP protocol.....	12
2.4 Access to the Certification Revocation List (CRL) via LDAP protocol.....	12
2.5 Access to the Certification Revocation List (CRL) via OCSP protocol.....	12
2.6 Time Stamp access.....	12
3. Policies for issuance and management of user's certificates for universal electronic signature.....	13
3.1.1. Description of the certificate for universal electronic signature Spektar Personal Universal Certificate.....	13
3.1.2. Application of the certificate for universal electronic signature Spektar Personal Universal Certificate .....	13
3.1.3. Identification of the issuance and management policy of the certificate for universal electronic signature Spektar Personal Universal Certificate.....	14
3.1.4. Profile of the certificate for universal electronic signature Spektar Personal Universal Certificate.....	14
3.1.5. Operating rules for issuance and management of the certificate for universal electronic signature Spektar Personal Universal Certificate.....	16
3.1.5.1 Application forms .....	16
3.1.5.2. Certificate issuance.....	17
3.1.5.3 Certificate publishing .....	18
3.1.5.4 Acceptance of the certificate.....	18
3.1.5.5 Suspension and renewal of certificates.....	19
3.1.5.5.1 Suspension of the certificate.....	19
3.1.5.5.2 Renewal of suspended certificates.....	20
3.1.5.6 Certificate renewal.....	20
3.1.5.7 Certificate revocation .....	23
3.2.1. Description of the certificate for universal electronic signature Spektar Personal Restricted Universal Certificate.....	24
3.2.2. Application of the certificate for universal electronic signature Spektar Personal Restricted Universal Certificate .....	24
3.2.3. Identification of the issuance and management policy of the certificate for universal electronic signature Spektar Personal Restricted Universal Certificate.....	25
3.2.4. Profile of the certificate for universal electronic signature Spektar Personal Restricted Universal Certificate.....	25
3.2.5. Operating rules for issuance and management of the certificate for universal electronic signature Spektar Personal Restricted Universal Certificate.....	27
3.2.5.1 Application forms .....	27
3.2.5.2. Certificate issuance.....	28
3.2.5.3 Certificate publishing .....	29
3.2.5.4 Acceptance of the certificate by the Owner, Signatory, respectively.....	29

3.2.5.5 Suspension and renewal of certificates.....	30
3.2.5.5.1 Suspension of the certificate.....	30
3.2.5.5.2 Renewal of suspended certificates.....	31
3.2.5.6 Certificate renewal.....	31
3.2.5.7 Certificate revocation .....	34
3.3.1. Description of the certificate for universal electronic signature Spektar Org Universal Certificate.....	35
3.3.2. Application of the certificate for universal electronic signature Spektar Org Universal Certificate .....	35
3.3.3. Identification of the issuance and management policy of the certificate for universal electronic signature Spektar Org Universal Certificate.....	36
3.3.4. Profile of the certificate for universal electronic signature Spektar Org Universal Certificate.....	36
3.3.5. Operating rules for issuance and management of the certificate for universal electronic signature Spektar Org Universal Certificate.....	38
3.3.5.1 Application forms .....	38
3.3.5.2. Certificate issuance.....	40
3.3.5.3 Certificate publishing .....	40
3.3.5.4 Acceptance of the certificate by the Owner, Signatory, respectively.....	41
3.3.5.5 Suspension and renewal of certificates.....	41
3.3.5.5.1 Suspension of the certificate.....	41
3.3.5.5.2 Renewal of suspended certificates.....	42
3.3.5.6 Certificate renewal.....	43
3.3.5.7 Certificate revocation .....	46
3.4.1. Description of the certificate for universal electronic signature Spektar Org Restricted Universal Certificate.....	46
3.4.2. Application of the certificate for universal electronic signature Spektar Org Restricted Universal Certificate .....	47
3.4.3. Identification of the issuance and management policy of the certificate for universal electronic signature Spektar Org Restricted Universal Certificate.....	48
3.4.4. Profile of the certificate for universal electronic signature Spektar Org Restricted Universal Signature.....	48
3.4.5. Operating rules for issuance and management of the certificate for universal electronic signature Spektar Org Restricted Universal Certificate.....	50
3.4.5.1 Application forms .....	50
3.4.5.2. Certificate issuance.....	52
3.4.5.4 Acceptance of the certificate by the Owner, Signatory, respectively.....	53
3.4.5.5 Suspension and renewal of certificates.....	53
3.4.5.5.1 Suspension of the certificate.....	53
3.4.5.5.2 Renewal of suspended certificates.....	54
3.4.5.6 Certificate renewal.....	55
3.4.5.7 Certificate revocation .....	58
4.1.1. Description of the certificate for advanced electronic signature Spektar Personal NonUniversal Certificate.....	59
4.1.2. Application of the certificate for advanced electronic signature Spektar Personal NonUniversal Certificate .....	59
4.1.3. Identification of the issuance and management policy of the certificate for advanced electronic signature Spektar Personal NonUniversal Certificate.....	60
4.1.4. Profile of the certificate for advanced electronic signature Spektar Personal NonUniversal Certificate.....	60
4.1.5. Operating rules for issuance and management of the certificate for advanced electronic signature Spektar Personal NonUniversal Certificate.....	62
4.1.5.1 Application forms .....	62

4.1.5.2. Certificate issuance.....	63
4.1.5.3 Certificate publishing .....	64
4.1.5.4 Certificate acceptance by the Owner, Signatory, respectively.....	64
4.1.5.5 Suspension and renewal of certificates.....	64
4.1.5.5.1 Suspension of the certificate for advanced electronic signature.....	64
4.1.5.5.2 Renewal of suspended certificates.....	66
4.1.5.6 Certificate renewal.....	66
4.1.5.7 Certificate revocation .....	69
4.2.1. Description of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate.....	70
4.2.2. Application of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate .....	70
4.2.3. Identification of the issuance and management policy of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate.....	71
4.2.4. Profile of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate.....	71
4.2.5. Operating rules for issuance and management of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate.....	73
4.2.5.1 Application forms .....	73
4.2.5.2. Certificate issuance.....	74
4.2.5.3 Certificate publishing .....	75
4.2.5.4 Certificate acceptance by the Owner, Signatory, respectively.....	75
4.2.5.5 Suspension and renewal of certificates.....	76
4.2.5.5.1 Suspension of the certificate for advanced electronic signature.....	76
4.2.5.5.2 Renewal of suspended certificates.....	77
4.2.5.6 Certificate renewal.....	77
4.2.5.7 Certificate revocation .....	80

## 1. Introduction

This document contains the policies followed by *Spektar AD* as a certification services provider (CSPProvider) for issuance and management of certificates for universal and advanced electronic signature and is drawn up in accordance with the requirements of EDESA, sublegislation on its application and the recommendations 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 these of „Designing and managing a Windows Public Key Infrastructure“.

The document describes the services offered by the CSPProvider and the procedures for issuance, suspension, renewal and revocation of certificates.

*Certificate policy* is part of the *User's Manual* and has the effect of general rules and regulations for the provision of certification services by the CSPProvider.

## 2. Services offered

*Spektar AD* as a certification services provider offers the following services connected with issuance and management of certificates for electronic signature:

- issues and manages certificates for universal electronic signature to physical persons and organizations/traders;
- issues and manages certificates for advanced electronic signature to physical persons and organizations/traders;
- provides third parties with different methods of access to the public electronic registry with issued, suspended or revoked certificates;
- verifies the date and time of a given Hash-identifier of a signed electronic document.

### 2.1 Certificate issuance and management

The certificate for universal electronic signature is an electronic document, signed by a registered certification services provider, which certifies the relation between Owner/Signatory and a public key held by him. The certificate for universal electronic signature is used for identification of the Owner/Signatory in cases such as document signing, access to information systems or information encipherment.

According to the ordinances of the EDESA only the universal electronic signature has the effect of a hand-written signature to all addressees. The certificates for universal electronic signature issued by registered certification services providers have the effect of a hand-written signature before state or local authorities.

Certificates for advanced electronic signature are signed by a certification services provider electronic documents, containing certain properties and certifying the relation between the Owner/Signatory and a public key held by him for checking signed documents and objects and give possibility for identification of the Owner/Signatory.

The CSPProvider certifies upon written request by the Owner and Signatory. The order for submission of requests for a certificate, the necessary documents to be attached and the requirements are described in the policies for each particular type of certificate.

### **2.1.1 Issued user's certificates**

The CSPProvider issues different types of user's certificates for universal and advanced electronic signature depending on the purpose of the certificate and persons who can request certificates. Certificates issued by the CSPProvider are for either personal or official use.

#### **2.1.1.1 Personal certificates for universal electronic signature**

**Spektar Personal Universal Certificate** - issued to physical persons Owner and Signatory. This certificate has the effect of a certificate for universal electronic signature. It can be used for identification purposes when accessing Internet applications, protected communications and electronic signing of all kinds of documents.

**Spektar Personal Restricted Universal Certificate** - issued to physical persons Owner and Signatory. This certificate has the effect of a certificate for universal electronic signature. It can be used for identification purposes when accessing Internet applications, protected communications and electronic signing of documents. Electronic documents accompanied with this certificate can be addressed only to state or local authorities.

#### **2.1.1.2 Certificates for universal electronic signature for official use**

**Spektar Org Universal Certificate** – issued to an Owner - organization/trader and Signatory – physical person. This certificate has the effect of a certificate for universal electronic signature. It can be used for identification purposes when accessing Internet applications, protected communications and electronic signing of all kinds of documents.

**Spektar Org Restricted Universal Certificate** - issued to Owner – organization/trader and Signatory – physical person. This certificate has the effect of a certificate for universal electronic signature. It can be used for identification purposes when accessing Internet applications, protected communications and electronic signing of documents. Electronic documents accompanied with this certificate can be addressed only to state or local authorities.

#### **2.1.1.3 Personal certificate for advanced electronic signature**

**Spektar Personal NonUniversal Certificate** – issued to physical persons Owner and Signatory. This certificate has the effect of a certificate for advanced electronic signature. It can be used for identification purposes when accessing Internet applications, protected communications and electronic signing of all kinds of documents.

#### 2.1.1.4 Certificate for advanced electronic signature for official use

**Spektar Org NonUniversal Certificate** - issued to an Owner - organization/trader and Signatory – physical person. It is not necessary the Signatory to be an employee in the organization of the Owner. This certificate has the effect of a certificate for advanced electronic signature. It can be used for identification purposes when accessing Internet applications, protected communications and electronic signing of all kinds of documents.

#### 2.1.2 Basic certificate of the CSPProvider

The basic certificate *Spektar Root CA* of the certification services provider *Spektar AD* is a self-signed and issued certificate for universal electronic signature and is valid for 20 years.

The operating certificates *Spektar Universal CA* and *Spektar NonUniversal CA* of the Certification Authority (CA) of the CSPProvider are signed with the basic private key of *Spektar Root CA*

Profile of the basic certificate *Spektar CA* of the CSPProvider:

Version	V3	
Serial number	[serial number]	
Signature Algorithm	Sha1RSA	
Valid from	[dd Month gggg hh:mm:ss]	
Validit to	[dd Month gggg hh:mm:ss]	
Issuer	CN	Spektar Root CA
	Phone	+359 2 9699 200
	E	ca@spektar.org
	PostalCode	1000
	STREET	11A Carnegie Street
	OU	Spektar CA
	O	Spektar JSC, B: 831431323
	L	Sofia
	S	Sofia
	C	BG

Subject	CN	Spektar Root CA
	Phone	+359 2 9699 200
	E	ca@spektar.org
	PostalCode	1000
	STREET	11A Carnegie Street
	OU	Spektar CA
	O	Spektar JSC, B: 831431323
	L	Sofia
	S	Sofia
	C	BG
Public Key	RSA(4096 Bits)	
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing	
Subject Key Identifier	[XXX...]	
CA Version	V0.0	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.18463.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.spektar.org/repository/cps">http://www.spektar.org/repository/cps</a>	
Basic Constraints	Subject Type=CA Path Length Constraint=None	
Thumbprint algorithm	sha1	
Thumbprint	[XXX...]	

### 2.1.3 Operating certificate for universal electronic signature of the CSPProvider *Spektar Universal CA*

The operating certificate for universal electronic signature of the Certification Authority *Spektar Universal CA* is signed with the basic private key of the CSPProvider and is valid for 5 years.

All issued by the CSPProvider certificates for universal electronic signature of the type: *Spektar Universal* and *Spektar Restricted Universal* are signed with the private operating key of *Spektar Universal CA*.

Profile of the operating certificate *Spektar Universal CA* of the CSPProvider:

Version	V3
Serial number	[serial number]
Signature Algorithm	Sha1RSA
Valid from	[dd Month gggg hh:mm:ss]
Validit to	[dd Month gggg hh:mm:ss]

Issuer	CN	Spektar Root CA
	Phone	+359 2 9699 200
	E	ca@spektar.org
	PostalCode	1000
	STREET	11A Carnegie Street
	OU	Spektar CA
	O	Spektar" JSC, B: 831431323
	L	Sofia
	S	Sofia
	C	BG
Subject	CN	Spektar Universal CA
	Phone	+359 2 9699 200
	E	ca@spektar.org
	PostalCode	1000
	STREET	11A Carnegie Street
	OU	Spektar CA
	O	Spektar JSC, B: 831431323
	L	Sofia
	S	Sofia
	C	BG
Public Key	RSA(1024 Bits)	
Subject Key Identifier	[XXX...]	
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing	
CA Version	V0.0	
Certificate Policies	<p>[1]Certificate Policy:  Policy Identifier=1.3.6.1.4.1.18463.1.1.1  [1,1]Policy Qualifier Info:  Policy Qualifier Id=CPS  Qualifier:  <a href="http://www.spektar.org/repository/cps">http://www.spektar.org/repository/cps</a></p>	
Certificate Template Name	SubCA	
Authority Key Identifier	KeyID=[XXX...]	
CRL Distribution Points	<p>[1]CRL Distribution Point  Distribution Point Name:  Full Name:  URL=<a href="http://www.spektar.org/repository/crl/Spektar Root CA.crl">http://www.spektar.org/repository/crl/Spektar Root CA.crl</a></p>	
Authority Information Access	<p>[1]Authority Info Access  Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)  Alternative Name:  URL=<a href="http://www.spektar.org/repository/aia/Spektar Root CA.crt">http://www.spektar.org/repository/aia/Spektar Root CA.crt</a>  [2]Authority Info Access  Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)  Alternative Name:  URL=<a href="http://ocsp.spektar.org/">http://ocsp.spektar.org/</a></p>	
Basic Constraints	Subject Type=CA	

	Path Length Constraint=None
Thumbprint algorithm	sha1
Thumbprint	[XXX...]

#### 2.1.4 Identification of the policies for issuance and management of certificates for universal electronic signature

Each policy for issuance of certificates of universal electronic signature is given an Object Identifier (OID). The values of the object identifiers for the certificates for universal electronic signature issued by the CSPProvider are:

Type of the certificate for universal electronic signature	Object Identifier
Spektar Personal Universal Certificate	1.3.6.1.4.1.18463.1.1.1.1
Spektar Personal Restricted Universal Certificate	1.3.6.1.4.1.18463.1.1.1.2
Spektar Org Universal Certificate	1.3.6.1.4.1.18463.1.1.1.3
Spektar Org Restricted Universal Certificate	1.3.6.1.4.1.18463.1.1.1.4

#### 2.1.5 Operating certificate for advanced electronic signature *Spektar NonUniversal CA*

The operating certificate for advanced electronic signature of the Certification Authority Spektar NonUniversal CA is signed with the basic private key of the CSPProvider and is valid for 5 years.

All issued by the CSPProvider certificates for advanced electronic signature of the *Spektar NonUniversal* type are signed with the private operating key of *Spektar NonUniversal CA*.

Profile of the operating certificate *Spektar NonUniversal CA* of the CSPProvider:

Version	V3	
Serial number	[serial number]	
Signature Algorithm	Sha1RSA	
Valid from	[dd Month gggg hh:mm:ss]	
Valid to	[dd Month gggg hh:mm:ss]	
Issuer	CN	Spektar Root CA
	Phone	+359 2 9699 200
	E	ca@spektar.org
	PostalCode	1000
	STREET	11A Carnegie Street
	OU	Spektar CA
	O	Spektar JSC, B: 831431323
	L	Sofia
	S	Sofia
C	BG	

Subject	E	ca@spektar.org
	CN	Spektar NonUniversal CA
	OU	Spektar CA
	O	Spektar JSC, B: 831431323
	L	Sofia
	S	Sofia
	C	BG
Public Key	RSA(1024 Bits)	
Subject Key Identifier	[XXX...]	
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing	
CA Version	V0.0	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.18463.1.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.spektar.org/repository/cps">http://www.spektar.org/repository/cps</a>	
Certificate Template Name	SubCA	
Authority Key Identifier	KeyID=[XXX...]	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= <a href="http://www.spektar.org/repository/crl/Spektar Root CA.crl">http://www.spektar.org/repository/crl/Spektar Root CA.crl</a>	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= <a href="http://www.spektar.org/repository/aia/Spektar Root CA.crt">http://www.spektar.org/repository/aia/Spektar Root CA.crt</a> [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= <a href="http://ocsp.spektar.org/">http://ocsp.spektar.org/</a>	
Basic Constraints	Subject Type=CA Path Length Constraint=None	
Thumbprint algorithm	sha1	
Thumbprint	[XXX...]	

### 2.1.6 Identification of the policies for issuance of certificates for advanced electronic signature

Each policy for issuance of certificates of advanced electronic signature is given an Object Identifier (OID). The values of the object identifiers for the certificates for advanced electronic signature issued by the CSPProvider are:

Type of the certificate for advanced electronic signature	Object Identifier
Spektar Personal NonUniversal Certificate	1.3.6.1.4.1.18463.1.1.2.1
Spektar Org NonUniversal Certificate	1.3.6.1.4.1.18463.1.1.2.2

## 2.2 Maintenance of an electronic public registry

The CSPProvider keeps an electronic *Public Registry* according to the X 509 standard. The CSPProvider publishes in the registry its basic and operating certificates as well as the certificates issued to physical persons and organizations/traders. The following is also published in the registry:

- *Certificate Practice Statement*;
- *Certificate Policy*;
- Certification Revocation List (CRL) of the CSPProvider;
- other documents and information according to the operating legislation.

A detailed description of the frequency of registry updates and control of the access to the registry can be found in the Certificate Practice Statement (Section 2.3).

## 2.3 Access to the Certification Revocation List (CRL) via HTTP protocol

The certification revocation list is part of the electronic public registry of the CSPProvider. 24-hour /twenty-four hours/ free access to the list via HTTP (Hyper Text Transfer Protocol) is given.

To access via HTTP protocol one needs to send a request to the server for directory services of the CSPProvider on the website: <http://www.spektar.org> .

## 2.4 Access to the Certification Revocation List (CRL) via LDAP protocol

The certification revocation list is part of the electronic public registry of the CSPProvider. 24-hour /twenty-four hours/ free access to the list via LDAP (Lightweight Directory Access Protocol) is given.

To access via LDAP protocol one needs to send a request to the server for directory services of the CSPProvider on the website: <ldap://www.spektar.org> .

## 2.5 Access to the Certification Revocation List (CRL) via OCSP protocol

The CSPProvider offers the possibility for status check for the certificates issued in real time by using OCSP protocol (On-line Certificate Status Protocol).

This service allows the Relying Parties to receive information on the status of a particular certificate at the moment of enquiry.

To use the OCSP access the Relying Party needs specialized software (OCSP client). Information on settings for access to the OCSP services offered can be found on the CSPProvider's website: <http://www.spektar.org> .

## 2.6 Time Stamp access

The CSPProvider can verify the date and time of presentation of the Hash-identifier of a signed electronic document. (TimeStamping).

The time certificate for time verifies the precise date and time at which the client's electronic document is registered in the TimeStamp server of the CSPProvider. The TimeStamp server of the CSPProvider gives a serial number and signs electronically the time certificate.

### **3. Policies for issuance and management of user's certificates for universal electronic signature**

#### **3.1. Certificate for universal electronic signature *Spektar Personal Universal Certificate***

##### **3.1.1. Description of the certificate for universal electronic signature *Spektar Personal Universal Certificate***

*Spektar Personal Universal Certificate* is issued to an Owner Organization/Trader and Signatory - physical person and certifies their identity and their relation to the public key.

*Spektar Personal Universal Certificate* is a certificate for universal electronic signature. Every electronic signature accompanied by this certificate has the meaning of a handwritten signature and assures authenticity, integrity, confidentiality and irrevocability of the signed messages.

The private-public key pair which corresponds to the certificate for universal electronic signature is generated and kept on a smart card and there is no possibility to extract the private key from the card.

The certificate for universal electronic signature is valid for 1 /one/ year.

##### **3.1.2. Application of the certificate for universal electronic signature *Spektar Personal Universal Certificate***

The certificate for universal electronic signature and the corresponding private-public key pair can be used for:

- 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.

*Spektar Personal Universal Certificate* can be used to identify the Owner and the Signatory when using personal electronic mail, access to secured information systems and electronic commerce. The corresponding key pair can be used to put electronic signature and to encipher data.

Checks for the purpose and validity of *Spektar Personal Universal Certificate* are run using the following data in the profile of the certificate for universal electronic signature:

- policy according to which the certificate for universal electronic signature is issued – shown in the *Certificate Policy* field;
- purpose and restrictions of the certificate for universal electronic signature – described in the *Key Usage, Enhanced Key Usage* and *Application Policies* fields;
- data of Owner and Signatory in the certificate for universal electronic signature – shown in the *Subject* field.

The relying party has the obligation to check the purpose and applicability of the *Spektar Personal Universal Certificate* before accepting an electronic signature accompanied by the certificate for universal electronic signature.

### 3.1.3. Identification of the issuance and management policy of the certificate for universal electronic signature *Spektar Personal Universal Certificate*

The policy for issuance and management of *Spektar Personal Universal Certificate* is designated with Object Identifier (OID) with the following value:

<b>OID= 1.3.6.1.4.1.18463.1.1.1.1</b>
---------------------------------------

According to the requirements of the Activities of CSProviders the policy for issuance and management of *Spektar Personal Universal Certificate* is an integral part of the User's Manual and is published on the following internet address: <http://www.spektar.org>

### 3.1.4. Profile of the certificate for universal electronic signature *Spektar Personal Universal Certificate*

Version	V3	
Serial number	[serial number]	
Signature Algorithm	Sha1RSA	
Issuer	Phone	+359 2 9699 200
	E	<a href="mailto:ca@spektar.org">ca@spektar.org</a>
	PostalCode	1000
	Street	11A, Carnegie Street
	CN	Spektar Universal CA
	OU	Spektar CA
	O	Spektar JSC, B:831431323
	L	Sofia
	S	Sofia
	C	BG
Valid from	[dd Month gggg hh:mm:ss]	
Validit to	[dd Month gggg hh:mm:ss]	

Subject	CN	Signatory's name in full
	O	Owner's name in full [NT:name]
	OU*	Owner's Personal Identification Number* [EGNT: Personal Identification Number (as well as indication of its nationality) or date of birth (yymmdd)]
	OU	Spektar Personal Universal Certificate
	STREET	Owner's address [str.,No,block,entr.,floor,flat,town,country*]
	L	Region of the address of the Owner [region]
	PostalCode	Postal code of the address of the Owner
	S	Address of residence of the Signatory [str.,No,block,entr.,floor,flat,town,country*]
	C	Country [XX]
	E	E-mail address of the Owner for which the certificate for universal electronic signature is issued
	Phone	Phone number of the Owner [+35912312341234]
Public Key Type/Length	RSA (1024 Bits)	
Key Usage (critical)	Digital signature Key Encipherment Data Encipherment Key Agreement Non-repudiation	
SMIME Capabilities	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7	
Subject Key Identifier	[XXX...]	
Authority Key Identifier	Key ID=[XXX...]	
CRL Distribution Points	URL=ldap:///CN=Spektar Universal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDistributionPoint URL=http://www.spektar.org/repository/crl/Spektar Universal CA.crl	
Authority Information Access	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///CN=Spektar Universal CA,CN=AIA,	

	DC=spektar,DC=org?cACertificate?base?objectClass=certificationAuthority URL=http://www.spektar.org/repository/aia/Spektar Universal CA.crt  Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.spektar.org/
Certificate Template Information	Template=SpektarPersonalUniversal
Enhanced Key Usage	Document Signing (1.3.6.1.4.1.311.10.3.12) SpektarPersonalUniversalPolicy (1.3.6.1.4.1.18463.1.1.1.1) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	Policy Identifier=1.3.6.1.4.1.18463.1.1.1.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.spektar.org/repository/cps">http://www.spektar.org/repository/cps</a>
Application Policies	[1]Application Certificate Policy: Policy Identifier=Document Signing [2]Application Certificate Policy: Policy Identifier=SpektarPersonalUniversalPolicy(1.3.6.1.4.1.18463.1.1.1.1) [3]Application Certificate Policy: Policy Identifier=Client Authentication [4]Application Certificate Policy: Policy Identifier=Secure Email
Thumbprint Algorithm	Sha1
Thumbprint	[XXX...]
Issuer Alternate Name	[hyperlink to the registration of the CSPProvider in CRC]

*Fields marked \* are optional.*

### 3.1.5. Operating rules for issuance and management of the certificate for universal electronic signature *Spektar Personal Universal Certificate*

#### 3.1.5.1 Application forms

The person applying for a certificate for universal electronic signature *Spektar Personal Universal Certificate*, further called Applicant, fills in properly and gives to the Registration Authority in person or via mail the following documents:

- application form for issuance and management of universal electronic signature (Form 2.7);
- certification services contract (2 copies);
- certification services application form (Form 3).
- data of the Signatory – physical person (Form 4.2)
- personally signed by hand copy of the personal identity card or passport of the Owner and text

saying: **'I agree the copy of my personal identity card to be used for the purposes of the CSPProvider'**

This consent is required by the Personal Data Protection Act.

The applicant can download the mentioned application forms from the following internet address: <http://www.spektar.org>

In case the application documents are not handed in person by the signatories to a representative of the Registration Authority, the documents need to be notarized.

After the CSPProvider signs the certification services contract a copy of it is sent to the Applicant by mail, with advice of delivery to the contact address given by the Applicant.

The Registration Authority checks the authenticity of the data given by the Applicant within 5 /five/ working days from the date of receiving the application documents.

The identity check includes:

- check for lack of documents required and for incorrectly filled in documents;
- identification of the Owner/Signatory of the certificate;
- authenticity of the data given.

In case of a refusal for issuance of a certificate for universal electronic signature the Registration Authority informs the Applicant by chosen by him means of communication and gives reason for refusal.

Via web-based interface the Signatory can follow and manage the issuance and management processes for the certificate for universal electronic signature.

### **3.1.5.2. Certificate issuance**

After the Signatory has confirmed his consent with the content of the DN (the information he gave for certification) and thus accepts the content of the public part of the *Subject* field he advances to the next procedure which is generation of a private-public key pair and submission of an electronic application form. All electronic applications for issuance of certificate for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the application. The electronic application is in PKCS#10 format which allows the Registration Authority of the CSPProvider to make sure that the Signatory holds the private key.

Through its Registration Authority the CSPProvider takes measures to authenticate the owner of the private key and to establish the fact that this private key is held by the Signatory accordingly

to the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In case of established correspondence the Registration Authority of the CSPProvider approves the application for universal electronic signature. The Certification Authority confirms and issues *Spektar Personal Universal Certificate*.

In case of established lack of correspondence the Applicant is informed by selected suitable means given by him for contact.

The certificate is not issued before the user pays for the service.

After certificate issuance the CSPProvider informs the Owner/Signatory and provides a way for them to receive it. The certificate for universal electronic signature can be accessed by loading it via the website of the CSPProvider <http://www.spektar.org>

### **3.1.5.3 Certificate publishing**

The certificate for universal electronic signature issued by the Certification Authority of the CSPProvider is published right after its generation in the electronic register of the provider.

The electronic register of the CSPProvider is public and ways of access are described in the *Certification Practice Statement* (Section 2.3).

### **3.1.5.4 Acceptance of the certificate**

The Owner or the Signatory can put a claim for incorrect content within a period 3 /three/ days after loading and installment of the certificate for universal electronic signature.

If after this period of time the Owner or Signatory has not put a claim for incorrect content, the certificate is considered accepted.

The certificate for universal electronic signature is considered accepted by the Owner and Signatory if before the above-stated period of 3 /three/ days it is used at least once.

### 3.1.5.5 Suspension and renewal of certificates

#### 3.1.5.5.1 Suspension of the certificate

Suspension of issued by the CSProvider certificates for universal electronic signatures follows the presence of certain reasons and the suspension period depends on the circumstances which caused the suspension. This period can not be more than 48 hours from the moment of suspension.

Application for suspension of the certificate for universal electronic signature can be submitted to the CSProvider in one of the following ways:

- by phone: +359 2 9699200/252

people applying for suspension shall give:

their names in full;

the phone number from which they are calling to suspend the certificate for universal electronic signature; /this phone is used for control/;

serial number of the certificate for universal electronic signature they wish to suspend;

reasons for the suspension request.

When requesting suspension the Owner/Signatory has to give his identification password from the application for certificate for universal electronic signature.

- by electronic mail

the person requesting the suspension downloads the *Certificate Suspension Application* from the CSProvider's website (Form 8);

fills in the form (Form 8) and sends it as an attachment in electronic mail to: [delovodstvo@spektar.org](mailto:delovodstvo@spektar.org)

When this person is the Owner/Signatory, he has to give the identification password from the application for certificate for universal electronic signature.

- through the CSProvider's website

the applicant fills in and sends electronic form *Certificate Suspension Application* (Form8).

- in person at CSProvider

the person requesting suspension at the CSProvider's office in person fills in *Certificate Suspension Application* (Form 8).

The CSProvider suspends the certificate for universal electronic signature and moves it to the certificate revocation list with status *HOLD*.

The CSPProvider identifies but does not certify the identity of the person requesting the certificate suspension.

The CSPProvider immediately notifies the Owner/Signatory of the certificate suspension.

#### **3.1.5.5.2 Renewal of suspended certificates**

Suspended certificates for universal electronic signature are renewed if within the legal framework of maximum 48-hours period of time the Owner submits a duly filled in and signed *Renewal of Suspended Certificates Application* (Form 9).

The *Renewal of Suspended Certificates Application* (Form 9) is filled in by the Owner when the reason for suspension no longer exists and assures the CSPProvider that he found out the reason for suspension as well as that the request for renewal is because of that finding.

In cases when the request for suspension rises from the Communications Regulation Commission, the CSPProvider gives the commission a copy of the written application for renewal.

The renewal is done by taking the certificate with *HOLD* status out of the certificate revocation list (CRL) in the CSPProvider's electronic register.

If after the legal 48 /forty-eight/-hours period of time from the certificate suspension there is no reason for its revocation, the CSPProvider automatically renews the certificate.

#### **3.1.5.6 Certificate renewal**

Certificates for universal electronic signature which are not revoked can be renewed before their validity expires without the necessity to generate another key pair.

The CSPProvider as a certification services provider allows the renewal of a certificate for universal electronic signature by using the existing key pair only once with the purpose of reducing the risk of its discredit.

In the *Certification Practice Statement* (Section 4) there is a detailed description of the methods for renewal of the certificate for universal electronic signature and some security arguments to be considered by the Signatory in his deciding on a specific choice.

**The procedure for renewal of the certificate for universal electronic signature without**

**generating a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;

The documents have to be notarized if they are not submitted in person to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check for correct content of the application form;
- identification of the Owner/Signatory;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Owner/Signatory and advances to renewal of the certificate for universal electronic signature.

After the Owner/Signatory confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation and submission of an electronic application. All electronic applications for issuance of certificates for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSPProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held in accordance with the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for universal electronic signature. The Certification Authority renews the requested *Spektar Personal Universal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for universal electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for universal electronic signature the CSProvider informs the Owner/Signatory that the access to the renewed *Spektar Personal Universal Certificate* is open and provides means for this access. The certificate for universal electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSProvider <http://www.spektar.org>

**The procedure for renewal of the certificate for universal electronic signature with generation of a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;

The documents have to be notarized if they are not submitted in person to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check for correct content of the application form;
- identification of the Owner/Signatory;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Owner/Signatory and advances to renewal of the certificate for universal electronic signature.

After the user confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation of a new private-public key pair and generation and submission of an electronic application. All electronic applications for issuance of certificates for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held in accordance with the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for universal electronic signature. The Certification Authority renews the requested *Spektar Personal Universal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for universal electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for universal electronic signature the CSPProvider informs the Owner/Signatory that the access to the renewed *Spektar Personal Universal Certificate* is open and provides means for this access. The certificate for universal electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSPProvider <http://www.spektar.org>

#### **3.1.5.7 Certificate revocation**

- revocation of the certificate for universal electronic signature with expired validity

If there is no application by the Owner/Signatory up to 10 /ten/ days before the expiry date of the certificate for universal electronic signature, the certificate for universal electronic signature is revoked automatically on its expiry date.

- revocation of the certificate for universal electronic signature before its expiry date

The certificate is revoked in cases of termination of the legal person of the certification services provider with no transfer to another certification services provider.

The certification services provider revokes the certificate in case of death or prohibition of the Owner/Signatory.

The certification services provider revokes the certificate in case of established incorrect data on the basis of which the certificate was issued.

The certificate is revoked before its expiry date if this is requested by the Owner/Signatory, in person or by mail. Certificate Revocation Application form (Form 10) is needed and it can be downloaded from the internet address <http://www.spektar.org>

In case the application form is not submitted in person it has to be notarized.

After establishing the identity and running additional checks for authenticity of the information given the Registration Authority inputs an electronic application form for status change of the user's certificate. The Certification Authority revokes the certificate by including it in the CRL.

### 3.2. Certificate for universal electronic signature *Spektar Personal Restricted Universal Certificate*

#### **3.2.1. Description of the certificate for universal electronic signature *Spektar Personal Restricted Universal Certificate***

*Spektar Personal Restricted Universal Certificate* - issued to physical persons Owner and Signatory and certifies their identity and their relation to the public key.

*Spektar Personal Restricted Universal Certificate* is a certificate for universal electronic signature. Every electronic signature accompanied by this certificate has the meaning of a handwritten signature and assures authenticity, integrity, confidentiality and irrevocability of the signed messages and can be addressed only to state or local authorities.

The private-public key pair which corresponds to the certificate for universal electronic signature is generated and kept on a smart card and there is no possibility to extract the private key from the card.

The certificate for universal electronic signature is valid for 1 /one/ year.

#### **3.2.2. Application of the certificate for universal electronic signature *Spektar Personal Restricted Universal Certificate***

The certificate for universal electronic signature and the corresponding private-public key pair can be used for:

- 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.

*Spektar Personal Restricted Universal Certificate* can be used to identify the Owner and the Signatory when using personal electronic mail, access to secured information systems and electronic commerce. The corresponding key pair can be used to put electronic signature and to encipher data.

Checks for the purpose and validity of *Spektar Personal Restricted Universal Certificate* are run using the following data in the profile of the certificate for universal electronic signature:

- policy according to which the certificate for universal electronic signature is issued – shown in the *Certificate Policy* field;

- purpose and restrictions of the certificate for universal electronic signature – described in the *Key Usage, Enhanced Key Usage* and *Application Policies* fields;
- data of Owner and Signatory in the certificate for universal electronic signature – shown in the *Subject* field.

The relying party has the obligation to check the purpose and applicability of the *Spektar Personal Universal Restricted Certificate* before accepting an electronic signature accompanied by the certificate for universal electronic signature.

### 3.2.3. Identification of the issuance and management policy of the certificate for universal electronic signature *Spektar Personal Restricted Universal Certificate*

The policy for issuance and management of *Spektar Personal Restricted Universal Certificate* is designated with Object Identifier (OID) with the following value:

OID= 1.3.6.1.4.1.18463.1.1.1.2
--------------------------------

According to the requirements of the Activities of CSPProviders the policy for issuance and management of *Spektar Personal Restricted Universal Certificate* is an integral part of the User's Manual and is published on the following internet address: <http://www.spektar.org>

### 3.2.4. Profile of the certificate for universal electronic signature *Spektar Personal Restricted Universal Certificate*

Version	V3	
Serial number	[serial number]	
Signature Algorithm	Sha1RSA	
Issuer	Phone	+359 2 9699 200
	E	<a href="mailto:ca@spektar.org">ca@spektar.org</a>
	PostalCode	1000
	Street	11A, Carnegie Street
	CN	Spektar Universal CA
	OU	Spektar CA
	O	Spektar JSC, B:831431323
	L	Sofia
	S	Sofia
	C	BG
Valid from	[dd Month gggg hh:mm:ss]	
Validit to	[dd Month gggg hh:mm:ss]	

Subject	CN	Signatory's name in full
	O	Owner's name in full [NT:name]
	OU*	Owner's Personal Identification Number* [EGNT: Personal Identification Number (as well as indication of its nationality) or date of birth (yymmdd)]
	OU	Spektar Personal Restricted Universal Certificate
	STREET	Owner's address [str.,No,block,entr.,floor,flat,town,country*]
	L	Region of the address of the Owner [region]
	PostalCode	Postal code of the address of the Owner
	S	Address of residence of the Signatory [str.,No,block,entr.,floor,flat,town,country*]
	C	Country [XX]
	E	E-mail address of the Signatory for which the certificate for universal electronic signature is issued
	Phone	Phone number of the Signatory [+35912312341234]
Public Key Type/Length	RSA (1024 Bits)	
Key Usage (critical)	Digital signature Key Encipherment Data Encipherment Key Agreement Non-repudiation	
SMIME Capabilities	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7	
Subject Key Identifier	[XXX...]	
Authority Key Identifier	Key ID=[XXX...]	
CRL Distribution Points	URL=ldap:///CN=Spektar Universal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDistributionPoint URL=http://www.spektar.org/repository/crl/Spektar Universal CA.crl	
Authority Information Access	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///CN=Spektar Universal CA,CN=AIA,	

	DC=spektar,DC=org?cACertificate?base?objectClass=certificationAuthority URL=http://www.spektar.org/repository/aia/Spektar Universal CA.crt  Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.spektar.org/
Certificate Template Information	Template=SpektarPersonalRestrictedUniversal
Enhanced Key Usage	Document Signing (1.3.6.1.4.1.311.10.3.12) SpektarPersonalRestrictedUniversalPolicy (1.3.6.1.4.1.18463.1.1.1.2) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	Policy Identifier=1.3.6.1.4.1.18463.1.1.1.2.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.spektar.org/repository/cps">http://www.spektar.org/repository/cps</a>
Application Policies	[1]Application Certificate Policy: Policy Identifier=Document Signing [2]Application Certificate Policy: Policy Identifier=SpektarPersonalRestrictedUniversalPolicy(1.3.6.1.4.1.18463.1.1.1.2) [3]Application Certificate Policy: Policy Identifier=Client Authentication [4]Application Certificate Policy: Policy Identifier=Secure Email
Thumbprint Algorithm	Sha1
Thumbprint	[XXX...]
Issuer Alternate Name	[hyperlink to the registration of the CSPProvider in CRC]

*Fields marked \* are optional.*

### 3.2.5. Operating rules for issuance and management of the certificate for universal electronic signature *Spektar Personal Restricted Universal Certificate*

#### 3.2.5.1 Application forms

The person applying for a certificate for universal electronic signature *Spektar Personal Restricted Universal Certificate*, further called Applicant, fills in properly and gives to the Registration Authority in person or via mail the following documents:

- application form for issuance and management of universal electronic signature (Form 2.8);
- certification services contract (2 copies);

- certification services application form (Form 3).
- data of the Signatory – physical person (Form 4.2)
- personally signed by hand copy of the personal identity card or passport of the Owner and text saying: **‘I agree the copy of my personal identity card to be used for the purposes of the CSPProvider’**

This consent is required by the Personal Data Protection Act.

The applicant can download the mentioned application forms from the following internet address: <http://www.spektar.org>

In case the application documents are not handed in person by the signatories to a representative of the Registration Authority, the documents need to be notarized.

After the CSPProvider signs the certification services contract a copy of it is sent to the Applicant by mail, with advice of delivery to the contact address given by the Applicant.

The Registration Authority checks the authenticity of the data given by the Applicant within 5 /five/ working days from the date of receiving the application documents.

The identity check includes:

- check for lack of documents required and for incorrectly filled in documents;
- identification of the Owner/Signatory of the certificate;
- authenticity of the data given.

In case of a refusal for issuance of a certificate for universal electronic signature the Registration Authority informs the Applicant by chosen by him means of communication and gives reason for refusal.

Via web-based interface the Signatory can follow and manage the issuance and management processes for the certificate for universal electronic signature.

### **3.2.5.2. Certificate issuance**

After the Signatory has confirmed his consent with the content of the DN (the information he gave for certification) and thus accepts the content of the public part of the *Subject* field he advances to the next procedure which is generation of a private-public key pair and submission of an electronic application form. All electronic applications for issuance of certificate for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the application. The electronic application is in PKCS#10 format which allows the

Registration Authority of the CSPProvider to make sure that the Signatory holds the private key.

Through its Registration Authority the CSPProvider takes measures to authenticate the owner of the private key and to establish the fact that this private key is held by the Signatory accordingly to the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In case of established correspondence the Registration Authority of the CSPProvider approves the application for universal electronic signature. The Certification Authority confirms and issues *Spektar Personal Restricted Universal Certificate*.

In case of established lack of correspondence the Applicant is informed by selected suitable means given by him for contact.

The certificate is not issued before the user pays for the service.

After certificate issuance the CSPProvider informs the Owner/Signatory and provides a way for them to receive it. The certificate for universal electronic signature can be accessed by loading it via the website of the CSPProvider <http://www.spektar.org>

### **3.2.5.3 Certificate publishing**

The certificate for universal electronic signature issued by the Certification Authority of the CSPProvider is published right after its generation in the electronic register of the provider.

The electronic register of the CSPProvider is public and ways of access are described in the *Certification Practice Statement* (Section 2.3).

### **3.2.5.4 Acceptance of the certificate by the Owner, Signatory, respectively**

The Owner/Signatory can put a claim for incorrect content within a period 3 /three/ days after loading and installment of the certificate for universal electronic signature.

If after this period of time the Owner/Signatory has not put a claim for incorrect content, the certificate is considered accepted.

The certificate for universal electronic signature is considered accepted by the Owner/Signatory if

before the above-stated period of 3 /three/ days it is used at least once.

### 3.2.5.5 Suspension and renewal of certificates

#### 3.2.5.5.1 Suspension of the certificate

Suspension of issued by the CSProvider certificates for universal electronic signatures follows the presence of certain reasons and the suspension period depends on the circumstances which caused the suspension. This period can not be more than 48 hours from the moment of suspension.

Application for suspension of the certificate for universal electronic signature can be submitted to the CSProvider in one of the following ways:

- by phone: +359 2 9699200/252

people applying for suspension shall give:

their names in full;

the phone number from which they are calling to suspend the certificate for universal electronic signature; /this phone is used for control/;

serial number of the certificate for universal electronic signature they wish to suspend;

reasons for the suspension request.

When requesting suspension the Owner/Signatory has to give his identification password from the application for certificate for universal electronic signature.

- by electronic mail

the person requesting the suspension downloads the *Certificate Suspension Application* from the CSProvider's website (Form 8);

fills in the form (Form 8) and sends it as an attachment in electronic mail to:  
[delovodstvo@spektar.org](mailto:delovodstvo@spektar.org)

When this person is the Owner/Signatory, he has to give the identification password from the application for certificate for universal electronic signature.

- through the CSProvider's website

the applicant fills in and sends electronic form *Certificate Suspension Application* (Form8).

- in person at CSProvider

the person requesting suspension at the CSProvider's office in person fills in *Certificate Suspension Application* (Form 8).

The CSProvider suspends the certificate for universal electronic signature and moves it to the certificate revocation list with status *HOLD*.

The CSPProvider identifies but does not certify the identity of the person requesting the certificate suspension.

The CSPProvider immediately notifies the Owner/Signatory of the certificate suspension.

#### **3.2.5.5.2 Renewal of suspended certificates**

Suspended certificates for universal electronic signature are renewed if within the legal framework of maximum 48-hours period of time the Owner submits a duly filled in and signed *Renewal of Suspended Certificates Application* (Form 9).

The *Renewal of Suspended Certificates Application* (Form 9) is filled in by the Owner when the reason for suspension no longer exists and assures the CSPProvider that he found out the reason for suspension as well as that the request for renewal is because of that finding.

In cases when the request for suspension rises from the Communications Regulation Commission, the CSPProvider gives the commission a copy of the written application for renewal.

The renewal is done by taking the certificate with *HOLD* status out of the certificate revocation list (CRL) in the CSPProvider's electronic register.

If after the legal 48 /forty-eight/-hours period of time from the certificate suspension there is no reason for its revocation, the CSPProvider automatically renews the certificate.

#### **3.2.5.6 Certificate renewal**

Certificates for universal electronic signature which are not revoked can be renewed before their validity expires without the necessity to generate another key pair.

The CSPProvider as a certification services provider allows the renewal of a certificate for universal electronic signature by using the existing key pair only once with the purpose of reducing the risk of its discredit.

In the *Certification Practice Statement* (Section 4) there is a detailed description of the methods for renewal of the certificate for universal electronic signature and some security arguments to be considered by the Signatory in his deciding on a specific choice.

**The procedure for renewal of the certificate for universal electronic signature without generating a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;

The documents have to be notarized if they are not submitted in person to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check for correct content of the application form;
- identification of the Owner/Signatory;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Owner/Signatory and advances to renewal of the certificate for universal electronic signature.

After the Owner/Signatory confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation and submission of an electronic application. All electronic applications for issuance of certificates for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSPProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held in accordance with the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for universal electronic signature. The Certification Authority renews the requested *Spektar Personal Restricted Universal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for universal electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for universal electronic signature the CSProvider informs the Owner/Signatory that the access to the renewed *Spektar Personal Restricted Universal Certificate* is open and provides means for this access. The certificate for universal electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSProvider <http://www.spektar.org>

**The procedure for renewal of the certificate for universal electronic signature with generation of a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;

The documents have to be notarized if they are not submitted in person to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check for correct content of the application form;
- identification of the Owner/Signatory;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Owner/Signatory and advances to renewal of the certificate for universal electronic signature.

After the user confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation of a new private-public key pair and generation and submission of an electronic application. All electronic applications for issuance of certificates for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSPProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held in accordance with the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for universal electronic signature. The Certification Authority renews the requested *Spektar Personal Restricted Universal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for universal electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for universal electronic signature the CSPProvider informs the Owner/Signatory that the access to the renewed *Spektar Personal Restricted Universal Certificate* is open and provides means for this access. The certificate for universal electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSPProvider <http://www.spektar.org>

### **3.2.5.7 Certificate revocation**

- revocation of the certificate for universal electronic signature with expired validity

If there is no application by the Owner/Signatory up to 10 /ten/ days before the expiry date of the certificate for universal electronic signature, the certificate for universal electronic signature is revoked automatically on its expiry date.

- revocation of the certificate for universal electronic signature before its expiry date

The certificate is revoked in cases of termination of the legal person of the certification services provider with no transfer to another certification services provider.

The certification services provider revokes the certificate in case of death or prohibition of the Owner/Signatory.

The certification services provider revokes the certificate in case of established incorrect data on the basis of which the certificate was issued.

The certificate is revoked before its expiry date if this is requested by the Owner/Signatory, in person

or by mail. Certificate Revocation Application form (Form 10) is needed and it can be downloaded from the internet address <http://www.spektar.org>

In case the application form is not submitted in person it has to be notarized.

After establishing the identity and running additional checks for authenticity of the information given the Registration Authority inputs an electronic application form for status change of the user's certificate. The Certification Authority revokes the certificate by including it in the CRL.

### **3.3. Certificate for universal electronic signature *Spektar Org Universal Certificate***

#### **3.3.1. Description of the certificate for universal electronic signature *Spektar Org Universal Certificate***

*Spektar Org Universal Certificate* is issued to an Owner Organization/Trader and Signatory - physical person and certifies their identity and their relation to the public key.

*Spektar Org Universal Certificate* is a certificate for universal electronic signature. Every electronic signature accompanied by this certificate has the meaning of a handwritten signature and assures authenticity, integrity, confidentiality and irrevocability of the signed messages.

The private-public key pair which corresponds to the certificate for universal electronic signature is generated and kept on a smart card and there is no possibility to extract the private key from the card.

The certificate for universal electronic signature is valid for 1 /one/ year.

#### **3.3.2. Application of the certificate for universal electronic signature *Spektar Org Universal Certificate***

The certificate for universal electronic signature and the corresponding private-public key pair can be used for:

- 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.

*Spektar Org Universal Certificate* can be used to identify the Owner and the Signatory when using personal electronic mail, access to secured information systems and electronic commerce. The corresponding key pair can be used to put electronic signature and to encipher data.

Checks for the purpose and validity of *Spektar Org Universal Certificate* are run using the following data in the profile of the certificate for universal electronic signature:

- policy according to which the certificate for universal electronic signature is issued – shown in the *Certificate Policy* field;
- purpose and restrictions of the certificate for universal electronic signature – described in the *Key Usage, Enhanced Key Usage* and *Application Policies* fields;
- data of Owner and Signatory in the certificate for universal electronic signature – shown in the *Subject* field.

The relying party has the obligation to check the purpose and applicability of the *Spektar Org Universal Certificate* before accepting an electronic signature accompanied by the certificate for universal electronic signature.

### 3.3.3. Identification of the issuance and management policy of the certificate for universal electronic signature *Spektar Org Universal Certificate*

The policy for issuance and management of *Spektar Org Universal Certificate* is designated with Object Identifier (OID) with the following value:

<b>OID=</b> 1.3.6.1.4.1.18463.1.1.1.3
---------------------------------------

According to the requirements of the Activities of CSPProviders the policy for issuance and management of *Spektar Org Universal Certificate* is an integral part of the User's Manual and is published on the following internet address: <http://www.spektar.org>

### 3.3.4. Profile of the certificate for universal electronic signature *Spektar Org Universal Certificate*

Version	V3	
Serial number	[serial number]	
Signature Algorithm	Sha1RSA	
Issuer	Phone	+359 2 9699 200
	E	<a href="mailto:ca@spektar.org">ca@spektar.org</a>
	PostalCode	1000
	Street	11A, Carnegie Street
	CN	Spektar Universal CA
	OU	Spektar CA
	O	Spektar JSC, B:831431323
	L	Sofia
	S	Sofia
C	BG	
Valid from	[dd Month gggg hh:mm:ss]	
Validit to	[dd Month gggg hh:mm:ss]	

Subject	CN	Signatory's name in full
	T	Reason for representative powers of the Signatory [capacity,N:notary public number. Letter of attorney number/dd.mm.yyyy, EGN:Personal Identification Number]
	O	Name of organization/trader
	OU	Court or other registration*
	OU	Identification number*,BULSTAT number*, VAT number* (if there is tax number registration) [B:Identification number, BULSTAT number, D:*VAT number]
	OU	Spektar Org Universal Certificate
	STREET	Management address of the Owner as in the current state certificate or in a document for creation [str.,No,block,entr.,floor,flat,town,country*]
	L	Region of the management address of the Owner [region]
	PostalCode	Postal code of the management address of the Owner
	S	Work address of the Signatory [str.,No,block,entr.,floor,flat,town,country*]
	C	Country [XX]
	E	E-mail address of the Signatory for which the certificate for universal electronic signature is issued
Phone	Work phone number of the Signatory [+359 123 1234 1234]	
Public Key Type/Length	RSA (1024 Bits)	
Key Usage (critical)	Digital signature Key Encipherment Data Encipherment Key Agreement Non-repudiation	
SMIME Capabilities	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7	
Subject Key Identifier	[XXX...]	
Authority Key	Key ID=[XXX...]	

Identifier	
CRL Distribution Points	URL=ldap:///CN=Spektar Universal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDistributionPoint URL=http://www.spektar.org/repository/crl/Spektar Universal CA.crl
Authority Information Access	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///CN=Spektar Universal CA,CN=AIA, DC=spektar,DC=org?cACertificate?base?objectClass=certificationAuthority URL=http://www.spektar.org/repository/aia/Spektar Universal CA.crt  Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.spektar.org/
Certificate Template Information	Template=SpektarOrgUniversal
Enhanced Key Usage	Document Signing (1.3.6.1.4.1.311.10.3.12) SpektarOrgUniversalPolicy (1.3.6.1.4.1.18463.1.1.1.3) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	Policy Identifier=1.3.6.1.4.1.18463.1.1.1.3.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.spektar.org/repository/cps">http://www.spektar.org/repository/cps</a>
Application Policies	[1]Application Certificate Policy: Policy Identifier=Document Signing [2]Application Certificate Policy: Policy Identifier=SpektarOrgUniversalPolicy(1.3.6.1.4.1.18463.1.1.1.3) [3]Application Certificate Policy: Policy Identifier=Client Authentication [4]Application Certificate Policy: Policy Identifier=Secure Email
Thumbprint Algorithm	Sha1
Thumbprint	[XXX...]
Issuer Alternate Name	[hyperlink to the registration of the CSPProvider in CRC]

*Fields marked \* are optional.*

### 3.3.5. Operating rules for issuance and management of the certificate for universal electronic signature *Spektar Org Universal Certificate*

#### 3.3.5.1 Application forms

The person applying for a certificate for universal electronic signature *Spektar Org Universal Certificate*, further called Applicant, fills in properly and gives to the Registration Authority in person or

via mail the following documents:

- application form for issuance and management of universal electronic signature (Form 2.1);
- certification services contract (2 copies);
- certification services application form (Form 3).

Documents identifying the Owner – Organization/Trader:

- Owner's data - Organization/Trader (Form 4.1);
- Company decision or other document certifying the creation – original or notarized copy;
- current state certificate, issued within 30 (thirty) days before application – original or notarized copy;
- Copy of VAT number\* (if there is tax number registration), Identification number\* and BULSTAT number\*.

Documents identifying the Signatory:

- notarized letter of attorney (Form 13), with which the Owner authorizes the Signatory;
- personally signed by hand copy of the personal identity card or passport and text saying: **'I agree the copy of my personal identity card to be used for the purposes of the CSPProvider'**

This consent is required by the Personal Data Protection Act.

- Signatory's declaration (Form 15).

The applicant can download the mentioned application forms from the following internet address: <http://www.spektar.org>

In case the application documents are not handed in person by the signatories to a representative of the Registration Authority, the documents need to be notarized.

After the CSPProvider signs the certification services contract a copy of it is sent to the Applicant by mail, with advice of delivery to the contact address given by the Applicant.

The Registration Authority checks the authenticity of the data given by the Applicant within 5 /five/ working days from the date of receiving the application documents.

The identity check includes:

- check for lack of documents required and for incorrectly filled in documents;
- identification of the Owner and Signatory of the certificate;
- authenticity of the data given.

In case of a refusal for issuance of a certificate for universal electronic signature the Registration Authority informs the Applicant by chosen by him means of communication and gives reason for refusal.

Via web-based interface the Signatory can follow and manage the issuance and management processes for the certificate for universal electronic signature.

### **3.3.5.2. Certificate issuance**

After the Signatory has confirmed his consent with the content of the DN (the information he gave for certification) and thus accepts the content of the public part of the *Subject* field he advances to the next procedure which is generation of a private-public key pair and submission of an electronic application form. All electronic applications for issuance of certificate for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the application. The electronic application is in PKCS#10 format which allows the Registration Authority of the CSPProvider to make sure that the Signatory holds the private key.

Through its Registration Authority the CSPProvider takes measures to authenticate the owner of the private key and to establish the fact that this private key is held by the Signatory accordingly to the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In case of established correspondence the Registration Authority of the CSPProvider approves the application for universal electronic signature. The Certification Authority confirms and issues *Spektar Org Universal Certificate*.

In case of established lack of correspondence the Applicant is informed by selected suitable means given by him for contact.

The certificate is not issued before the user pays for the service.

After certificate issuance the CSPProvider informs the Owner, the Signatory, respectively, and provides a way for them to receive it. The certificate for universal electronic signature can be accessed by loading it via the website of the CSPProvider <http://www.spektar.org>

### **3.3.5.3 Certificate publishing**

The certificate for universal electronic signature issued by the Certification Authority of the CSPProvider is published right after its generation in the electronic register of the provider.

The electronic register of the CSPProvider is public and ways of access are described in the *Certification Practice Statement* (Section 2.3).

#### **3.3.5.4 Acceptance of the certificate by the Owner, Signatory, respectively**

The Owner or the Signatory can put a claim for incorrect content within a period 3 /three/ days after loading and installment of the certificate for universal electronic signature.

If after this period of time the Owner or Signatory has not put a claim for incorrect content, the certificate is considered accepted.

The certificate for universal electronic signature is considered accepted by the Owner and Signatory if before the above-stated period of 3 /three/ days it is used at least once.

#### **3.3.5.5 Suspension and renewal of certificates**

##### **3.3.5.5.1 Suspension of the certificate**

Suspension of issued by the CSPProvider certificates for universal electronic signatures follows the presence of certain reasons and the suspension period depends on the circumstances which caused the suspension. This period can not be more than 48 hours from the moment of suspension.

Application for suspension of the certificate for universal electronic signature can be submitted to the CSPProvider in one of the following ways:

- by phone: +359 2 9699200/252

people applying for suspension shall give:

their names in full;

the phone number from which they are calling to suspend the certificate for universal electronic signature; /this phone is used for control/;

serial number of the certificate for universal electronic signature they wish to suspend;

reasons for the suspension request.

When requesting suspension the Owner/Signatory has to give his identification password from the application for certificate for universal electronic signature.

- by electronic mail

the person requesting the suspension downloads the *Certificate Suspension Application* from the CSPProvider's website (Form 8);

fills in the form (Form 8) and sends it as an attachment in electronic mail to:

[delovodstvo@spektar.org](mailto:delovodstvo@spektar.org)

When this person is the Owner/Signatory, he has to give the identification password from the application for certificate for universal electronic signature.

- through the CSPProvider's website  
the applicant fills in and sends electronic form *Certificate Suspension Application (Form8)*.
- in person at CSPProvider  
the person requesting suspension at the CSPProvider's office in person fills in *Certificate Suspension Application (Form 8)*.

The CSPProvider suspends the certificate for universal electronic signature and moves it to the certificate revocation list with status *HOLD*.

The CSPProvider identifies but does not certify the identity of the person requesting the certificate suspension.

The CSPProvider immediately notifies the Owner/Signatory of the certificate suspension.

#### **3.3.5.5.2 Renewal of suspended certificates**

Suspended certificates for universal electronic signature are renewed if within the legal framework of maximum 48-hours period of time the Owner submits a duly filled in and signed *Renewal of Suspended Certificates Application (Form 9)*.

The *Renewal of Suspended Certificates Application (Form 9)* is filled in by the Owner when the reason for suspension no longer exists and assures the CSPProvider that he found out the reason for suspension as well as that the request for renewal is because of that finding.

In cases when the request for suspension rises from the Communications Regulation Commission, the CSPProvider gives the commission a copy of the written application for renewal.

The renewal is done by taking the certificate with *HOLD* status out of the certificate revocation list (CRL) in the CSPProvider's electronic register.

If after the legal 48 /forty-eight/-hours period of time from the certificate suspension there is no reason for its revocation, the CSPProvider automatically renews the certificate.

### 3.3.5.6 Certificate renewal

Certificates for universal electronic signature which are not revoked can be renewed before their validity expires without the necessity to generate another key pair.

The CSPProvider as a certification services provider allows the renewal of a certificate for universal electronic signature by using the existing key pair only once with the purpose of reducing the risk of its discredit.

In the *Certification Practice Statement* (Section 4) there is a detailed description of the methods for renewal of the certificate for universal electronic signature and some security arguments to be considered by the Signatory in his deciding on a specific choice.

**The procedure for renewal of the certificate for universal electronic signature without generating a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the following documents:

- *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;
- current state certificate, issued within 30 (thirty) days before application date – original or a notarized copy);
- confirmation by the Signatory, certifying his consent to continue to make electronic announcements with all other powers according to the authorization by the Owner (Signatory's Declaration – Form 15).

The documents have to be notarized if they are not submitted in person by the signatories to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check for lack of required documents and for correctly filled in information;
- identification of the Owner and Signatory of the certificate for universal electronic signature;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Signatory and advances to renewal of the certificate for universal electronic signature.

After the Signatory confirms his consent with the content of the DN (the information given by him for

certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation and submission of an electronic application. All electronic applications for issuance of certificates for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSPProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held by the Signatory in accordance with the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for universal electronic signature. The Certification Authority renews the requested *Spektar Org Universal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for universal electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for universal electronic signature the CSPProvider informs the Owner/Signatory that the access to the renewed *Spektar Org Universal Certificate* is open and provides means for this access. The certificate for universal electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSPProvider <http://www.spektar.org>

**The procedure for renewal of the certificate with generation of a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the following documents:

- Certificate Renewal Application (Form 6) – a copy on paper, signed by the Owner;
- current state certificate, issued within 30 (thirty) days before application date – original or a notarized copy);
- confirmation by the Signatory, certifying his consent to continue to make electronic announcements with all other powers according to the authorization by the Owner (Signatory's Declaration – Form 15).

The documents have to be notarized if they are not submitted in person by the signatories to a

representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the filled in documents are received.

The check includes:

- check for lack of any of the required documents and for correctly filled in information;
- identification of the Owner and Signatory of the certificate for universal electronic signature;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Signatory and advances to renewal of the certificate for universal electronic signature.

After the Signatory confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation of a new key pair and an electronic application. All electronic applications for issuance of certificates for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSPProvider through its Registration Authority takes measures for authentication of the private key owner and establishing the fact that this private key is held by the Signatory in accordance with the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for universal electronic signature. The Certification Authority renews the requested *Spektar Org Universal Certificate*.

In case of established lack of correspondence the Signatory is notified.

Certificates for universal electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for universal electronic signature the CSPProvider informs the Owner/Signatory that the access to the renewed *Spektar Org Universal Certificate* is open and provides means for this access. The certificate for universal electronic signature can be accessed via its loading

through the web-based interface of the certification services provider CSPProvider <http://www.spektar.org>

### **3.3.5.7 Certificate revocation**

- revocation of the certificate for universal electronic signature with expired validity

If there is no application by the Owner or Signatory up to 10 /ten/ days before the expiry date of the certificate for universal electronic signature, the certificate for universal electronic signature is revoked automatically on its expiry date.

- revocation of the certificate for universal electronic signature before its expiry date

The certificate is revoked in cases of termination of the legal person of the certification services provider with no transfer to another certification services provider.

- revocation of the certificate for universal electronic signature before its expiry date

The certificate is revoked in cases of termination of the legal person of the certification services provider with no transfer to another certification services provider.

The certification services provider revokes the certificate in case of death or prohibition of the Owner or Signatory; termination of the legal person of the Owner; termination of the representative authority of the Signatory regarding the Owner; establishing that the certificate is issued on the basis of incorrect data.

The certificate is revoked before its expiry date if this is requested by the Owner or Signatory, in person or by mail. Certificate Revocation Application form (Form 10) is needed and it can be downloaded from the internet address <http://www.spektar.org>

In case the application form is not submitted in person it has to be notarized.

After establishing the identity and running additional checks for authenticity of the information given the Registration Authority inputs an electronic application form for status change of the user's certificate. The Certification Authority revokes the certificate by including it in the CRL.

## **3.4. Certificate for universal electronic signature *Spektar Org Restricted Universal Certificate***

### **3.4.1. Description of the certificate for universal electronic signature *Spektar Org Restricted Universal Certificate***

*Spektar Org Restricted Universal Certificate* is issued to an Owner Organization/Trader and Signatory - physical person and certifies their identity and their relation to the public key.

*Spektar Org Restricted Universal Certificate* is a certificate for universal electronic signature. Every electronic signature accompanied by this certificate has the meaning of a handwritten signature and assures authenticity, integrity, confidentiality and irrevocability of the signed messages and can be addressed only to state or local authorities.

The private-public key pair which corresponds to the certificate for universal electronic signature is generated and kept on a smart card and there is no possibility to extract the private key from the card.

The certificate for universal electronic signature is valid for 1 /one/ year.

### **3.4.2. Application of the certificate for universal electronic signature *Spektar Org Restricted Universal Certificate***

The certificate for universal electronic signature and the corresponding private-public key pair can be used for:

- 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.

*Spektar Org Restricted Universal Certificate* can be used to identify the Owner and the Signatory when using personal electronic mail, access to secured information systems and electronic commerce. The corresponding key pair can be used to put electronic signature and to encipher data.

Checks for the purpose and validity of *Spektar Org Restricted Universal Certificate* are run using the following data in the profile of the certificate for universal electronic signature:

- policy according to which the certificate for universal electronic signature is issued – shown in the *Certificate Policy* field;
- purpose and restrictions of the certificate for universal electronic signature – described in the *Key Usage, Enhanced Key Usage* and *Application Policies* fields;
- data of Owner and Signatory in the certificate for universal electronic signature – shown in the *Subject* field.

The relying party has the obligation to check the purpose and applicability of the *Spektar Org Restricted Universal Certificate* before accepting an electronic signature accompanied by the certificate for universal electronic signature.

### 3.4.3. Identification of the issuance and management policy of the certificate for universal electronic signature *Spektar Org Restricted Universal Certificate*

The policy for issuance and management of *Spektar Org Universal Certificate* is designated with Object Identifier (OID) with the following value:

<b>OID= 1.3.6.1.4.1.18463.1.1.1.4</b>
---------------------------------------

According to the requirements of the Activities of CSPProviders the policy for issuance and management of *Spektar Org Restricted Universal Certificate* is an integral part of the User's Manual and is published on the following internet address: <http://www.spektar.org>

### 3.4.4. Profile of the certificate for universal electronic signature *Spektar Org Restricted Universal Signature*

Version	V3	
Serial number	[serial number]	
Signature Algorithm	Sha1RSA	
Issuer	Phone	+359 2 9699 200
	E	<a href="mailto:ca@spektar.org">ca@spektar.org</a>
	PostalCode	1000
	Street	11A, Carnegie Street
	CN	Spektar Universal CA
	OU	Spektar CA
	O	Spektar JSC, B:831431323
	L	Sofia
	S	Sofia
	C	BG
Valid from	[dd Month gggg hh:mm:ss]	
Validit to	[dd Month gggg hh:mm:ss]	

Subject	CN	Signatory's name in full
	T	Reason for representative powers of the Signatory [capacity,N:notary public number. Letter of attorney number/dd.mm.yyyy, EGN:Personal Identification Number]
	O	Name of organization/trader
	OU	Court or other registration*
	OU	Identification number*,BULSTAT number*, VAT number* (if there is tax number registration) [B:Identification number, BULSTAT number, D:*VAT number]
	OU	Spektar Org Restricted Universal Certificate
	STREET	Management address of the Owner as in the current state certificate or in a document for creation [str.,No,block,entr.,floor,flat,town,country*]
	L	Region of the management address of the Owner [region]
	PostalCode	Postal code of the management address of the Owner
	S	Work address of the Signatory [str.,No,block,entr.,floor,flat,town,country*]
	C	Country [XX]
	E	E-mail address of the Signatory for which the certificate for universal electronic signature is issued
Phone	Work phone number of the Signatory [+359 123 1234 1234]	
Public Key Type/Length	RSA (1024 Bits)	
Key Usage (critical)	Digital signature Key Encipherment Data Encipherment Key Agreement Non-repudiation	
SMIME Capabilities	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7	
Subject Key Identifier	[XXX...]	
Authority Key Identifier	Key ID=[XXX...]	

CRL Distribution Points	URL=ldap:///CN=Spektar Universal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDistributionPoint URL=http://www.spektar.org/repository/crl/Spektar Universal CA.crl
Authority Information Access	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///CN=Spektar Universal CA,CN=AIA, DC=spektar,DC=org?cACertificate?base?objectClass=certificationAuthority URL=http://www.spektar.org/repository/aia/Spektar Universal CA.crt  Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.spektar.org/
Certificate Template Information	Template=SpektarOrgRestrictedUniversal
Enhanced Key Usage	Document Signing (1.3.6.1.4.1.311.10.3.12) SpektarOrgRestrictedUniversalPolicy (1.3.6.1.4.1.18463.1.1.1.4) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	Policy Identifier=1.3.6.1.4.1.18463.1.1.1.4.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.spektar.org/repository/cps
Application Policies	[1]Application Certificate Policy: Policy Identifier=Document Signing [2]Application Certificate Policy: Policy Identifier=SpektarOrgRestrictedUniversalPolicy(1.3.6.1.4.1.18463.1.1.1.4) [3]Application Certificate Policy: Policy Identifier=Client Authentication [4]Application Certificate Policy: Policy Identifier=Secure Email
Thumbprint Algorithm	Sha1
Thumbprint	[XXX...]
Issuer Alternate Name	[hyperlink to the registration of the CSPProvider in CRC]

*Fields marked \* are optional.*

### 3.4.5. Operating rules for issuance and management of the certificate for universal electronic signature *Spektar Org Restricted Universal Certificate*

#### 3.4.5.1 Application forms

The person applying for a certificate for universal electronic signature *Spektar Org Restricted Universal Certificate*, further called Applicant, fills in properly and gives to the Registration Authority in

person or via mail the following documents:

- application form for issuance and management of universal electronic signature (Form 2.2);
- certification services contract (2 copies);
- certification services application form (Form 3).

Documents identifying the Owner – Organization/Trader:

- Owner's data - Organization/Trader (Form 4.1);
- Company decision or other document certifying the creation – original or notarized copy;
- current state certificate, issued within 30 (thirty) days before application – original or notarized copy;
- Copy of VAT number\* (if there is tax number registration), Identification number\* and BULSTAT number\*.

Documents identifying the Signatory:

- notarized letter of attorney (Form 14), with which the Owner authorizes the Signatory;
- personally signed by hand copy of the personal identity card or passport and text saying: **'I agree the copy of my personal identity card to be used for the purposes of the CSPProvider'**

This consent is required by the Personal Data Protection Act.

- Signatory's declaration (Form 15).

The applicant can download the mentioned application forms from the following internet address: <http://www.spektar.org>

In case the application documents are not handed in person by the signatories to a representative of the Registration Authority, the documents need to be notarized.

After the CSPProvider signs the certification services contract a copy of it is sent to the Applicant by mail, with advice of delivery to the contact address given by the Applicant.

The Registration Authority checks the authenticity of the data given by the Applicant within 5 /five/ working days from the date of receiving the application documents.

The identity check includes:

- check for lack of documents required and for incorrectly filled in documents;
- identification of the Owner and Signatory of the certificate for universal electronic signature;
- authenticity of the data given.

In case of a refusal for issuance of a certificate for universal electronic signature the Registration Authority informs the Applicant by chosen by him means of communication and gives

reason for refusal.

Via web-based interface the Signatory can follow and manage the issuance and management processes for the certificate for universal electronic signature.

#### **3.4.5.2. Certificate issuance**

After the Signatory has confirmed his consent with the content of the DN (the information he gave for certification) and thus accepts the content of the public part of the *Subject* field he advances to the next procedure which is generation of a private-public key pair and submission of an electronic application form. All electronic applications for issuance of certificate for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the application. The electronic application is in PKCS#10 format which allows the Registration Authority of the CSPProvider to make sure that the Signatory holds the private key.

Through its Registration Authority the CSPProvider takes measures to authenticate the owner of the private key and to establish the fact that this private key is held by the Signatory accordingly to the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In case of established correspondence the Registration Authority of the CSPProvider approves the application for universal electronic signature. The Certification Authority confirms and issues *Spektar Org Restricted Universal Certificate*.

In case of established lack of correspondence the Applicant is informed by selected suitable means given by him for contact.

The certificate is not issued before the user pays for the service.

After certificate issuance the CSPProvider informs the Owner, the Signatory, respectively, and provides a way for them to receive it. The certificate for universal electronic signature can be accessed by loading it via the website of the CSPProvider <http://www.spektar.org>

#### **3.4.5.3 Certificate publishing**

The certificate for universal electronic signature issued by the Certification Authority of the CSPProvider

is published right after its generation in the electronic register of the provider.

The electronic register of the CSProvider is public and ways of access are described in the *Certification Practice Statement* (Section 2.3).

#### **3.4.5.4 Acceptance of the certificate by the Owner, Signatory, respectively**

The Owner or the Signatory can put a claim for incorrect content within a period 3 /three/ days after loading and installment of the certificate for universal electronic signature.

If after this period of time the Owner or Signatory has not put a claim for incorrect content, the certificate is considered accepted.

The certificate for universal electronic signature is considered accepted by the Owner and Signatory if before the above-stated period of 3 /three/ days it is used at least once.

#### **3.4.5.5 Suspension and renewal of certificates**

##### **3.4.5.5.1 Suspension of the certificate**

Suspension of issued by the CSProvider certificates for universal electronic signatures follows the presence of certain reasons and the suspension period depends on the circumstances which caused the suspension. This period can not be more than 48 hours from the moment of suspension.

Application for suspension of the certificate for universal electronic signature can be submitted to the CSProvider in one of the following ways:

- by phone: +359 2 9699200/252

people applying for suspension shall give:

their names in full;

the phone number from which they are calling to suspend the certificate for universal electronic signature; /this phone is used for control/;

serial number of the certificate for universal electronic signature they wish to suspend;

reasons for the suspension request.

When requesting suspension the Owner/Signatory has to give his identification password from the application for certificate for universal electronic signature.

- by electronic mail

the person requesting the suspension downloads the *Certificate Suspension Application*

from the CSPProvider's website (Form 8);

fills in the form (Form 8) and sends it as an attachment in electronic mail to:  
[delovodstvo@spektar.org](mailto:delovodstvo@spektar.org)

When this person is the Owner/Signatory, he has to give the identification password from the application for certificate for universal electronic signature.

- through the CSPProvider's website  
the applicant fills in and sends electronic form *Certificate Suspension Application* (Form8).
- in person at CSPProvider  
the person requesting suspension at the CSPProvider's office in person fills in *Certificate Suspension Application* (Form 8).

The CSPProvider suspends the certificate for universal electronic signature and moves it to the certificate revocation list with status *HOLD*.

The CSPProvider identifies but does not certify the identity of the person requesting the certificate suspension.

The CSPProvider immediately notifies the Owner/Signatory of the certificate suspension.

#### **3.4.5.5.2 Renewal of suspended certificates**

Suspended certificates for universal electronic signature are renewed if within the legal framework of maximum 48-hours period of time the Owner submits a duly filled in and signed *Renewal of Suspended Certificates Application* (Form 9).

The *Renewal of Suspended Certificates Application* (Form 9) is filled in by the Owner when the reason for suspension no longer exists and assures the CSPProvider that he found out the reason for suspension as well as that the request for renewal is because of that finding.

In cases when the request for suspension rises from the Communications Regulation Commission, the CSPProvider gives the commission a copy of the written application for renewal.

The renewal is done by taking the certificate with *HOLD* status out of the certificate revocation list (CRL) in the CSPProvider's electronic register.

If after the legal 48 /forty-eight/-hours period of time from the certificate suspension there is no reason for its revocation, the CSPProvider automatically renews the certificate.

### 3.4.5.6 Certificate renewal

Certificates for universal electronic signature which are not revoked can be renewed before their validity expires without the necessity to generate another key pair.

The CSPProvider as a certification services provider allows the renewal of a certificate for universal electronic signature by using the existing key pair only once with the purpose of reducing the risk of its discredit.

In the *Certification Practice Statement* (Section 4) there is a detailed description of the methods for renewal of the certificate for universal electronic signature and some security arguments to be considered by the Signatory in his deciding on a specific choice.

**The procedure for renewal of the certificate for universal electronic signature without generating a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the following documents:

- *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;
- current state certificate, issued within 30 (thirty) days before application date – original or a notarized copy);
- confirmation by the Signatory, certifying his consent to continue to make electronic announcements with all other powers according to the authorization by the Owner (Signatory's Declaration – Form 15).

The documents have to be notarized if they are not submitted in person by the signatories to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check for lack of required documents and for correctly filled in information;
- identification of the Owner and Signatory of the certificate for universal electronic signature;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Signatory and advances to renewal of the certificate for universal electronic signature.

After the Signatory confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation and submission of an electronic application. All electronic applications for issuance of certificates for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held by the Signatory in accordance with the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSProvider approves the application for renewal of the certificate for universal electronic signature. The Certification Authority renews the requested *Spektar Org Restricted Universal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for universal electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for universal electronic signature the CSProvider informs the Owner/Signatory that the access to the renewed *Spektar Org Restricted Universal Certificate* is open and provides means for this access. The certificate for universal electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSProvider <http://www.spektar.org>

**The procedure for renewal of the certificate with generation of a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the following documents:

- Certificate Renewal Application (Form 6) – a copy on paper, signed by the Owner;
- current state certificate, issued within 30 (thirty) days before application date – original or a notarized copy);
- confirmation by the Signatory, certifying his consent to continue to make electronic announcements with all other powers according to the authorization by the Owner (Signatory's

Declaration – Form 15).

The documents have to be notarized if they are not submitted in person by the signatories to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the filled in documents are received.

The check includes:

- check for lack of any of the required documents and for correctly filled in information;
- identification of the Owner and Signatory of the certificate for universal electronic signature;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Signatory and advances to renewal of the certificate for universal electronic signature.

After the Signatory confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation of a new key pair and an electronic application. All electronic applications for issuance of certificates for universal electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSProvider through its Registration Authority takes measures for authentication of the private key owner and establishing the fact that this private key is held by the Signatory in accordance with the requested type of certificate for universal electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSProvider approves the application for renewal of the certificate for universal electronic signature. The Certification Authority renews the requested *Spektar Org Restricted Universal Certificate*.

In case of established lack of correspondence the Signatory is notified.

Certificates for universal electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for universal electronic signature the CSProvider informs the

Owner/Signatory that the access to the renewed *Spektar Org Restricted Universal Certificate* is open and provides means for this access. The certificate for universal electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSPProvider <http://www.spektar.org>

#### **3.4.5.7 Certificate revocation**

- revocation of the certificate for universal electronic signature with expired validity

If there is no application by the Owner or Signatory up to 10 /ten/ days before the expiry date of the certificate for universal electronic signature, the certificate for universal electronic signature is revoked automatically on its expiry date.

- revocation of the certificate for universal electronic signature before its expiry date

The certificate is revoked in cases of suspension of the legal person of the certification services provider with no transfer to another certification services provider.

- revocation of the certificate for universal electronic signature before its expiry date

The certificate is revoked in cases of termination of the legal person of the certification services provider with no transfer to another certification services provider.

The certification services provider revokes the certificate in case of death or prohibition of the Owner or Signatory; termination of the legal person of the Owner; termination of the representative authority of the Signatory regarding the Owner; establishing that the certificate is issued on the basis of incorrect data.

The certificate is revoked before its expiry date if this is requested by the Owner or Signatory, in person or by mail. Certificate Revocation Application form (Form 10) is needed and it can be downloaded from the internet address <http://www.spektar.org>

In case the application form is not submitted in person it has to be notarized.

After establishing the identity and running additional checks for authenticity of the information given the Registration Authority inputs an electronic application form for status change of the user's certificate. The Certification Authority revokes the certificate by including it in the CRL.

## **4. Policies for issuance and management of user's certificates for advanced electronic signature**

### **4.1. Certificate for advanced electronic signature *Spektar Personal NonUniversal Certificate***

#### **4.1.1. Description of the certificate for advanced electronic signature *Spektar Personal NonUniversal Certificate***

*Spektar Personal NonUniversal Certificate* is issued to physical persons - Owner and Signatory and certifies their identity and their relation to the public key.

*Spektar Personal NonUniversal Certificate* is a certificate for advanced electronic signature. Every electronic signature accompanied by this certificate is an advanced electronic signature and assures authenticity, integrity, confidentiality and irrevocability of the signed messages.

The private-public key pair which corresponds to the certificate is generated and kept on a smart card and there is no possibility to extract the private key from the card.

The certificate for advanced electronic signature is valid for 1 /one/ year.

#### **4.1.2. Application of the certificate for advanced electronic signature *Spektar Personal NonUniversal Certificate***

The certificate for advanced electronic signature and the corresponding private-public key pair can be used for:

- 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.

*Spektar Personal NonUniversal Certificate* can be used to identify the Owner/Signatory when using personal electronic mail, access to secured information systems and electronic commerce. The corresponding key pair can be used to put electronic signature and to encipher data.

Checks for the purpose and validity of *Spektar Personal NonUniversal Certificate* are run using the following data in the profile of the certificate for advanced electronic signature:

- policy according to which the certificate for advanced electronic signature is issued – shown in the *Certificate Policy* field;
- purpose and restrictions of the certificate for advanced electronic signature – described in the *Key Usage, Enhanced Key Usage* and *Application Policies* fields;
- data of Owner/Signatory in the certificate for advanced electronic signature – shown in the *Subject* field.

The relying party has the obligation to check the purpose and applicability of the *Spektar Personal NonUniversal Certificate* before accepting an electronic signature accompanied by the certificate.

#### 4.1.3. Identification of the issuance and management policy of the certificate for advanced electronic signature *Spektar Personal NonUniversal Certificate*

The policy for issuance and management of Spektar Org NonUniversal Certificate is designated with Object Identifier (OID) with the following value:

<b>OID=1.3.6.1.4.1.18463.1.1.2.1</b>
--------------------------------------

According to the requirements of the Activities of CSPProviders the policy for issuance and management of *Spektar Personal NonUniversal Certificate* is an integral part of the User's Manual and is published on the following internet address: <http://www.spektar.org>

#### 4.1.4. Profile of the certificate for advanced electronic signature *Spektar Personal NonUniversal Certificate*

<b>Version</b>	V3	
<b>Serial number</b>	[serial number]	
<b>Signature Algorithm</b>	Sha1RSA	
<b>Issuer</b>	Phone	+359 2 9699 200
	E	ca@spektar.org
	PostalCode	1000
	Street	11A, Carnegie Street
	CN	Spektar NonUniversal CA
	OU	Spektar CA
	O	Spektar JSC, B:831431323
	L	Sofia
	S	Sofia
C	BG	
<b>Valid from</b>	[dd Month gggg hh:mm:ss]	
<b>Validit to</b>	[dd Month gggg hh:mm:ss]	

<b>Subject</b>	CN	Signatory's name in full
	O	Owner's name in full [NT:name]
	OU*	Owner's Personal Identification Number* [EGNT: Personal Identification Number (as well as indication of its nationality) or date of birth (yymmdd)]
	OU	Spektar Personal NonUniversal Certificate
	STREET	Owner's address [str.,No,block,entr.,floor,flat,town,country*]
	L	Region of the address of the Owner [region]
	PostalCode	Postal code of the address of the Owner
	S	Address of residence of the Signatory [str.,No,block,entr.,floor,flat,town,country*]
	C	Country [XX]
	E	E-mail address of the Owner for which the certificate for advanced electronic signature is issued
	Phone	Phone number of the Owner [+35912312341234]
<b>Public Key Type/Length</b>	RSA (1024 Bits)	
<b>Key Usage (critical)</b>	Digital signature Key Encipherment Data Encipherment Key Agreement Non-repudiation	
<b>SMIME Capabilities</b>	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7	
<b>Subject Key Identifier</b>	[XXX...]	
<b>Authority Key Identifier</b>	Key ID=[XXX...]	
<b>CRL Distribution Points</b>	URL=ldap:///CN=Spektar NonUniversal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDistributionPoint URL=http://www.spektar.org/repository/crl/Spektar NonUniversal CA.crl	
<b>Authority Information Access</b>	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///CN=Spektar NonUniversal CA,CN=AIA, DC=spektar,DC=org?cACertificate?base?objectClass=certificationAuthority URL=http://www.spektar.org/repository/aia/Spektar NonUniversal CA.crt Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	

	Alternative Name: URL= <a href="http://ocsp.spektar.org/">http://ocsp.spektar.org/</a>
<b>Certificate Template Information</b>	Template=SpektarPersonalNonUniversal
<b>Enhanced Key Usage</b>	Document Signing (1.3.6.1.4.1.311.10.3.12) SpektarPersonalNonUniversalPolicy (1.3.6.1.4.1.18463.1.1.2.1) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
<b>Certificate Policies</b>	Policy Identifier=1.3.6.1.4.1.18463.1.1.2.1.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.spektar.org/repository/cps">http://www.spektar.org/repository/cps</a>
<b>Application Policies</b>	[1]Application Certificate Policy: Policy Identifier=Document Signing [2]Application Certificate Policy: Policy Identifier=SpektarPersonalNonUniversalPolicy(1.3.6.1.4.1.18463.1.1.2.1) [3]Application Certificate Policy: Policy Identifier=Client Authentication [4]Application Certificate Policy: Policy Identifier=Secure Email
<b>Thumbprint Algorithm</b>	Sha1
<b>Thumbprint</b>	[XXX...]
<b>Issuer Alternate Name</b>	[ <a href="#">hyperlink to the registration of the CSPProvider in CRC</a> ]

*Fields marked \* are optional.*

#### **4.1.5. Operating rules for issuance and management of the certificate for advanced electronic signature *Spektar Personal NonUniversal Certificate***

##### **4.1.5.1 Application forms**

The person applying for a certificate for advanced electronic signature *Spektar Personal NonUniversal Certificate*, further called Applicant, fills in properly and gives to the Registration Authority in person or via mail the following documents:

- application form for issuance and management of advanced electronic signature (Form 2.9);
- certification services contract (2 copies);
- certification services application form (Form 3).
- data of the Signatory – physical person (Form 4.2)
- personally signed by hand copy of the personal identity card or passport and text saying: **‘I agree the copy of my personal identity card to be used for the purposes of the CSPProvider’**

This consent is required by the Personal Data Protection Act.

The applicant can download the mentioned application forms from the following internet address: <http://www.spektar.org>

In case the application documents are not handed in person by the signatories to a

representative of the Registration Authority, the documents need to be notarized.

After the CSPProvider signs the certification services contract a copy of it is sent to the Applicant by mail, with advice of delivery to the contact address given by the Applicant.

The Registration Authority checks the authenticity of the data given by the Applicant within 5 /five/ working days from the date of receiving the application documents.

The identity check includes:

- check for lack of documents required and for incorrectly filled in documents;
- identification of the Owner/Signatory of the certificate;
- authenticity of the data given.

In case of a refusal for issuance of a certificate for advanced electronic signature the Registration Authority informs the Applicant by him means of communication chosen by him and gives reason for refusal.

Via web-based interface the Signatory can follow and manage the issuance and management processes for the certificate for advanced electronic signature.

#### **4.1.5.2. Certificate issuance**

After the Signatory has confirmed his consent with the content of the DN (the information he gave for certification) and thus accepts the content of the public part of the *Subject* field he advances to the next procedure which is generation of a private-public key pair and submission of an electronic application form. All electronic applications for issuance of certificate for advanced electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the application. The electronic application is in PKCS#10 format which allows the Registration Authority of the CSPProvider to make sure that the Signatory holds the private key.

Through its Registration Authority the CSPProvider takes measures to authenticate the owner of the private key and to establish the fact that this private key is held by the Signatory accordingly to the requested type of certificate for advanced electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In case of established correspondence the Registration Authority of the CSPProvider approves the

application for advanced electronic signature. The Certification Authority confirms and issues *Spektar Personal NonUniversal Certificate*.

In case of established lack of correspondence the Applicant is informed by selected suitable means given by him for contact.

The certificate is not issued before the user pays for the service.

After certificate issuance the CSPProvider informs the Owner/Signatory and provides a way for them to receive it. The certificate for advanced electronic signature can be accessed by loading it via the website of the CSPProvider <http://www.spektar.org>

#### **4.1.5.3 Certificate publishing**

The certificate for advanced electronic signature issued by the Certification Authority of the CSPProvider is published right after its generation in the electronic register of the provider.

The electronic register of the CSPProvider is public and ways of access are described in the *Certification Practice Statement* (Section 2.3).

#### **4.1.5.4 Certificate acceptance by the Owner, Signatory, respectively**

The Owner or the Signatory can put a claim for incorrect content within a period 3 /three/ days after loading and installment of the certificate for advanced electronic signature.

If after this period of time the Owner or Signatory has not put a claim for incorrect content, the certificate is considered accepted.

The certificate for advanced electronic signature is considered accepted by the Owner and Signatory if before the above-stated period of 3 /three/ days it is used at least once.

#### **4.1.5.5 Suspension and renewal of certificates**

##### **4.1.5.5.1 Suspension of the certificate for advanced electronic signature**

Suspension of issued by the CSPProvider certificates for advanced electronic signatures follows the presence of certain reasons and the suspension period depends on the circumstances which caused the suspension. This period can not be more than 48 hours from the moment of suspension.

Application for suspension of the certificate for advanced electronic signature can be submitted to the CSPProvider in one of the following ways:

- by phone: +359 2 9699200/252

people applying for suspension shall give:

their names in full;

the phone number from which they are calling to suspend the certificate for advanced electronic signature; /this phone is used for control/;

serial number of the certificate for advanced electronic signature they wish to suspend;

reasons for the suspension request.

When requesting suspension the Owner/Signatory has to give his identification password from the application for certificate for advanced electronic signature.

- by electronic mail

the person requesting the suspension downloads the *Certificate Suspension Application* from the CSPProvider's website (Form 8);

fills in the form (Form 8) and sends it as an attachment in electronic mail to: [delovodstvo@spektar.org](mailto:delovodstvo@spektar.org)

When this person is the Owner/Signatory, he has to give the identification password from the application for certificate for advanced electronic signature.

- through the CSPProvider's website

the applicant fills in and sends electronic form *Certificate Suspension Application* (Form8).

- in person at CSPProvider

the person requesting suspension at the CSPProvider's office in person fills in *Certificate Suspension Application* (Form 8).

The CSPProvider suspends the certificate for advanced electronic signature and moves it to the certificate revocation list with status *HOLD*.

The CSPProvider identifies but does not certify the identity of the person requesting the certificate suspension.

The CSPProvider immediately notifies the Owner/Signatory of the certificate suspension.

#### 4.1.5.5.2 Renewal of suspended certificates

Suspended certificates for advanced electronic signature are renewed if within the legal framework of maximum 48-hours period of time the Owner submits a duly filled in and signed *Renewal of Suspended Certificates Application* (Form 9).

The *Renewal of Suspended Certificates Application* (Form 9) is filled in by the Owner when the reason for suspension no longer exists and assures the CSPProvider that he found out the reason for suspension as well as that the request for renewal is because of that finding.

In cases when the request for suspension rises from the Communications Regulation Commission, the CSPProvider gives the commission a copy of the written application for renewal.

The renewal is done by taking the certificate with *HOLD* status out of the certificate revocation list (CRL) in the CSPProvider's electronic register.

If after the legal 48 /forty-eight/-hours period of time from the certificate suspension there is no reason for its revocation, the CSPProvider automatically renews the certificate.

#### 4.1.5.6 Certificate renewal

Certificates for advanced electronic signature which are not revoked can be renewed before their validity expires without the necessity to generate another key pair.

The CSPProvider as a certification services provider allows the renewal of a certificate for advanced electronic signature by using the existing key pair only once with the purpose of reducing the risk of its discredit.

In the *Certification Practice Statement* there is a detailed description of the methods for renewal of the certificate for advanced electronic signature and some security arguments to be considered by the Signatory in his deciding on a specific choice.

**The procedure for renewal of the certificate for advanced electronic signature without generating a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;

The documents have to be notarized if they are not submitted in person to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check correct content of the application form;
- identification of the Owner/Signatory;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Owner/Signatory and advances to renewal of the certificate for advanced electronic signature.

After the Owner/Signatory confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation and submission of an electronic application. All electronic applications for issuance of certificates for advanced electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSPProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held in accordance with the requested type of certificate for advanced electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for advanced electronic signature. The Certification Authority renews the requested *Spektar Personal NonUniversal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for advanced electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for advanced electronic signature the CSPProvider informs the Owner/Signatory that the access to the renewed *Spektar Personal NonUniversal Certificate* is open and

provides means for this access. The certificate for advanced electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSProvider <http://www.spektar.org>

**The procedure for renewal of the certificate for advanced electronic signature with generation of a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;

The documents have to be notarized if they are not submitted in person to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check correct content of the application form;
- identification of the Owner/Signatory;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Owner/Signatory and advances to renewal of the certificate for advanced electronic signature.

After the user confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation of a new private-public key pair and generation and submission of an electronic application. All electronic applications for issuance of certificates for advanced electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held in accordance with the requested type of certificate for advanced electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for advanced electronic signature. The Certification Authority renews the requested *Spektar Personal NonUniversal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for advanced electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for advanced electronic signature the CSPProvider informs the Owner/Signatory that the access to the renewed *Spektar Personal NonUniversal Certificate* is open and provides means for this access. The certificate for advanced electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSPProvider <http://www.spektar.org>

#### **4.1.5.7 Certificate revocation**

- revocation of the certificate for advanced electronic signature with expired validity

If there is no application by the Owner/Signatory up to 10 /ten/ days before the expiry date of the certificate for advanced electronic signature, the certificate for advanced electronic signature is revoked automatically on its expiry date.

- revocation of the certificate for advanced electronic signature before its expiry date

The certificate is revoked in cases of termination of the legal person of the certification services provider with no transfer to another certification services provider.

The certification services provider revokes the certificate in case of death or prohibition of the Owner/Signatory.

The certification services provider revokes the certificate in case of established incorrect data on the basis of which the certificate was issued.

The certificate is revoked before its expiry date if this is requested by the Owner/Signatory, in person or by mail. Certificate Revocation Application form (Form 10) is needed and it can be downloaded from the internet address <http://www.spektar.org>

In case the application form is not submitted in person it has to be notarized.

After establishing the identity and running additional checks for authenticity of the information given

the Registration Authority inputs an electronic application form for status change of the user's certificate. The Certification Authority revokes the certificate by including it in the CRL.

#### 4.2. Certificate for advanced electronic signature *Spektar Org NonUniversal Certificate*

##### **4.2.1. Description of the certificate for advanced electronic signature *Spektar Org NonUniversal Certificate***

*Spektar Org NonUniversal Certificate* is issued to a Signature Owner Organization/Trader and Signatory - physical person and certifies their identity and their relation to the public key.

*Spektar Org NonUniversal Certificate* is a certificate for advanced electronic signature. Every electronic signature accompanied by this certificate is an advanced electronic signature and assures authenticity, integrity, confidentiality and irrevocability of the signed messages.

The private-public key pair which corresponds to the certificate is generated and kept on a smart card and there is no possibility to extract the private key from the card.

The certificate for advanced electronic signature is valid for 1 /one/ year.

##### **4.2.2. Application of the certificate for advanced electronic signature *Spektar Org NonUniversal Certificate***

The certificate for advanced electronic signature and the corresponding private-public key pair can be used for:

- 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.

*Spektar Org NonUniversal Certificate* can be used to identify the Owner and the Signatory when using personal electronic mail, access to secured information systems and electronic commerce. The corresponding key pair can be used to put electronic signature and to encipher data.

Checks for the purpose and validity of *Spektar Org NonUniversal Certificate* are run using the following data in the profile of the certificate for advanced electronic signature:

- policy according to which the certificate for advanced electronic signature is issued – shown in the *Certificate Policy* field;
- purpose and restrictions of the certificate for advanced electronic signature – described in the *Key Usage, Enhanced Key Usage* and *Application Policies* fields;
- data of Owner/Signatory in the certificate for advanced electronic signature – shown in the *Subject* field.

The relying party has the obligation to check the purpose and applicability of the *Spektar Org NonUniversal Certificate* before accepting an electronic signature accompanied by the certificate.

#### 4.2.3. Identification of the issuance and management policy of the certificate for advanced electronic signature *Spektar Org NonUniversal Certificate*

The policy for issuance and management of Spektar Org NonUniversal Certificate is designated with Object Identifier (OID) with the following value:

**OID=** 1.3.6.1.4.1.18463.1.1.2.2

According to the requirements of the Activities of CSPProviders the policy for issuance and management of *Spektar Org NonUniversal Certificate* is an integral part of the User's Manual and is published on the following internet address: <http://www.spektar.org>

#### 4.2.4. Profile of the certificate for advanced electronic signature *Spektar Org NonUniversal Certificate*

<b>Version</b>	V3	
<b>Serial number</b>	[serial number]	
<b>Signature Algorithm</b>	Sha1RSA	
<b>Issuer</b>	Phone	+359 2 9699 200
	E	<a href="mailto:ca@spektar.org">ca@spektar.org</a>
	PostalCode	1000
	Street	11A, Carnegie Street
	CN	Spektar NonUniversal CA
	OU	Spektar CA
	O	Spektar JSC, B:831431323
	L	Sofia
	S	Sofia
C	BG	
<b>Valid from</b>	[dd Month gggg hh:mm:ss]	
<b>Validit to</b>	[dd Month gggg hh:mm:ss]	

<b>Subject</b>	CN	Signatory's name in full
	T	Reason for representative powers of the Signatory [capacity,N:notary public number. Letter of attorney number/dd.mm.yyyy, EGN:Personal Identification Number (as well as an indication of its nationality)]
	O	Name of organization/trader
	OU	Court or other registration
	OU	Identification number*,BULSTAT number*, VAT number* (if there is tax number registration) [B:Identification number, BULSTAT number, D:*VAT number]
	OU	Spektar Org NonUniversal Certificate
	STREET	Management address of the Owner as in the current state certificate or in a document for creation [str.,No,block,entr.,floor,flat,town,country*]
	L	Region of the management address of the Owner [region]
	PostalCode	Postal code of the management address of the Owner
	S	Work address of the Signatory [str.,No,block,entr.,floor,flat,town,country*]
	C	Country [XX]
	E	E-mail address of the Signatory for which the certificate for advanced electronic signature is issued
	Phone	Work phone number of the Signatory [+359 123 1234 1234]
<b>Public Key Type/Length</b>	RSA (1024 Bits)	
<b>Key Usage (critical)</b>	Digital signature Key Encipherment Data Encipherment Key Agreement Non-repudiation	
<b>SMIME Capabilities</b>	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7	
<b>Subject Key Identifier</b>	[XXX...]	
<b>Authority Key Identifier</b>	Key ID=[XXX...]	
<b>CRL Distribution Points</b>	URL=ldap:///CN=Spektar NonUniversal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDistributionPoint URL=http://www.spektar.org/repository/crl/Spektar NonUniversal CA.crl	

<b>Authority Information Access</b>	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///CN=Spektar NonUniversal CA,CN=AIA, DC=spektar,DC=org?cACertificate?base?objectClass=certificationAuthority URL=http://www.spektar.org/repository/aia/Spektar NonUniversal CA.crt  Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.spektar.org/
<b>Certificate Template Information</b>	Template=SpektarOrgNonUniversal
<b>Enhanced Key Usage</b>	Document Signing (1.3.6.1.4.1.311.10.3.12) SpektarOrgNonUniversalPolicy (1.3.6.1.4.1.18463.1.1.2.2) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
<b>Certificate Policies</b>	Policy Identifier=1.3.6.1.4.1.18463.1.1.2.2.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.spektar.org/repository/cps">http://www.spektar.org/repository/cps</a>
<b>Application Policies</b>	[1]Application Certificate Policy: Policy Identifier=Document Signing [2]Application Certificate Policy: Policy Identifier=SpektarOrgNonUniversalPolicy(1.3.6.1.4.1.18463.1.1.2.2) [3]Application Certificate Policy: Policy Identifier=Client Authentication [4]Application Certificate Policy: Policy Identifier=Secure Email
<b>Thumbprint Algorithm</b>	Sha1
<b>Thumbprint</b>	[XXX...]
<b>Issuer Alternate Name</b>	[hyperlink to the registration of the CSPProvider in CRC]

*Fields marked \* are optional*

#### **4.2.5. Operating rules for issuance and management of the certificate for advanced electronic signature *Spektar Org NonUniversal Certificate***

##### **4.2.5.1 Application forms**

The person applying for a certificate for advanced electronic signature *Spektar Org NonUniversal Certificate*, further called Applicant, fills in properly and gives to the Registration Authority in person or via mail the following documents:

- application form for issuance and management of advanced electronic signature (Form 2.3);
- certification services contract (2 copies);
- certification services application form (Form 3).

Documents identifying the Owner – Organization/Trader:

- Owner's data - Organization/Trader (Form 4.1);
- Company decision or other document certifying the creation – original or notarized copy;

- current state certificate, issued within 30 (thirty) days before application – original or notarized copy;
- Copy of VAT number\* (if there is tax number registration), Identification number\* and BULSTAT number\*.

Documents identifying the Signatory:

- notarized letter of attorney (Form 13), with which the Owner authorizes the Signatory;
- personally signed by hand copy of the personal identity card or passport and text saying: **‘I agree the copy of my personal identity card to be used for the purposes of the CSPProvider’**;

This consent is required by the Personal Data Protection Act.

- Signatory’s declaration (Form 15).

The applicant can download the mentioned application forms from the following internet address: <http://www.spektar.org>

In case the application documents are not handed in person by the signatories to a representative of the Registration Authority, the documents need to be notarized.

After the CSPProvider signs the certification services contract a copy of it is sent to the Applicant by mail, with advice of delivery to the contact address given by the Applicant.

The Registration Authority checks the authenticity of the data given by the Applicant within 5 /five/ working days from the date of receiving the application documents.

The identity check includes:

- check for lack of documents required and for incorrectly filled in documents;
- identification of the Owner and Signatory of the certificate;
- authenticity of the data given.

In case of a refusal for issuance of a certificate for advanced electronic signature the Registration Authority informs the Applicant by chosen by him means of communication and gives reason for refusal.

Via web-based interface the Signatory can follow and manage the issuance and management processes for the certificate for advanced electronic signature.

#### **4.2.5.2. Certificate issuance**

After the Signatory has confirmed his consent with the content of the DN (the information he gave for certification) and thus accepts the content of the public part of the *Subject* field he advances to the next procedure which is generation of a private-public key pair and submission of an electronic application

form. All electronic applications for issuance of certificate for advanced electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the application. The electronic application is in PKCS#10 format which allows the Registration Authority of the CSPProvider to make sure that the Signatory holds the private key.

Through its Registration Authority the CSPProvider takes measures to authenticate the owner of the private key and to establish the fact that this private key is held by the Signatory accordingly to the requested type of certificate for advanced electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In case of established correspondence the Registration Authority of the CSPProvider approves the application for advanced electronic signature. The Certification Authority confirms and issues *Spektar Org NonUniversal Certificate*.

In case of established lack of correspondence the Applicant is informed by selected suitable means given by him for contact.

The certificate is not issued before the user pays for the service.

After certificate issuance the CSPProvider informs the Owner, the Signatory, respectively, and provides a way for them to receive it. The certificate for advanced electronic signature can be accessed by loading it via the website of the CSPProvider <http://www.spektar.org>

#### **4.2.5.3 Certificate publishing**

The certificate for advanced electronic signature issued by the Certification Authority of the CSPProvider is published right after its generation in the electronic registry of the provider.

The electronic registry of the CSPProvider is public and ways of access are described in the *Certification Practice Statement* (Section 2.3).

#### **4.2.5.4 Certificate acceptance by the Owner, Signatory, respectively**

The Owner or the Signatory can put a claim for incorrect content within a period 3 /three/ days after loading and installment of the certificate for advanced electronic signature.

If after this period of time the Owner or Signatory has not put a claim for incorrect content, the certificate is considered accepted.

The certificate for advanced electronic signature is considered accepted by the Owner and Signatory if before the above-stated period of 3 /three/ days it is used at least once.

#### **4.2.5.5 Suspension and renewal of certificates**

##### **4.2.5.5.1 Suspension of the certificate for advanced electronic signature**

Suspension of issued by the CSPProvider certificates for advanced electronic signatures follows the presence of certain reasons and the suspension period depends on the circumstances which caused the suspension. This period can not be more than 48 hours from the moment of suspension.

Application for suspension of the certificate for advanced electronic signature can be submitted to the CSPProvider in one of the following ways:

- by phone: +359 2 9699200/252

people applying for suspension shall give:

their names in full;

the phone number from which they are calling to suspend the certificate for advanced electronic signature; /this phone is used for control/;

serial number of the certificate for advanced electronic signature they wish to suspend;

reasons for the suspension request.

When requesting suspension the Owner/Signatory has to give his identification password from the application for certificate for advanced electronic signature.

- by electronic mail

the person requesting the suspension downloads the *Certificate Suspension Application* from the CSPProvider's website (Form 8);

fills in the form (Form 8) and sends it as an attachment in electronic mail to: [delovodstvo@spektar.org](mailto:delovodstvo@spektar.org)

When this person is the Owner/Signatory, he has to give the identification password from the application for certificate for advanced electronic signature.

- through the CSPProvider's website

the applicant fills in and sends electronic form *Certificate Suspension Application* (Form8).

- in person at CSPProvider  
the person requesting suspension at the CSPProvider's office in person fills in *Certificate Suspension Application* (Form 8).

The CSPProvider suspends the certificate for advanced electronic signature and moves it to the certificate revocation list with status *HOLD*.

The CSPProvider identifies but does not certify the identity of the person requesting the certificate suspension.

The CSPProvider immediately notifies the Owner/Signatory of the certificate suspension.

#### **4.2.5.5.2 Renewal of suspended certificates**

Suspended certificates for advanced electronic signature are renewed if within the legal framework of maximum 48-hours period of time the Owner submits a duly filled in and signed *Renewal of Suspended Certificates Application* (Form 9).

The *Renewal of Suspended Certificates Application* (Form 9) is filled in by the Owner when the reason for suspension no longer exists and assures the CSPProvider that he found out the reason for suspension as well as that the request for renewal is because of that finding.

In cases when the request for suspension rises from the Communications Regulation Commission, the CSPProvider gives the commission a copy of the written application for renewal.

The renewal is done by taking the certificate with *HOLD* status out of the certificate revocation list (CRL) in the CSPProvider's electronic registry.

If after the legal 48 /forty-eight/-hours period of time from the certificate suspension there is no reason for its revocation, the CSPProvider automatically renews the certificate.

#### **4.2.5.6 Certificate renewal**

Certificates for advanced electronic signature which are not revoked can be renewed before their validity expires without the necessity to generate another key pair.

The CSPProvider as a certification services provider allows the renewal of a certificate for advanced electronic signature by using the existing key pair only once with the purpose of reducing the risk of its discredit.

In the *Certification Practice Statement* there is a detailed description of the methods for renewal of the certificate for advanced electronic signature and some security arguments to be considered by the Signatory in his deciding on a specific choice.

**The procedure for renewal of the certificate for advanced electronic signature without generating a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the following documents:

- *Certificate Renewal Application* (Form 6) – a copy on paper, signed by the Owner;
- current state certificate, issued within 30 (thirty) days before application date – original or a notarized copy);
- confirmation by the Signatory, certifying his consent to continue to make electronic announcements with all other powers according to the authorization by the Owner (Signatory's Declaration – Form 15).

The documents have to be notarized if they are not submitted in person by the signatories to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the application documents are received.

The check includes:

- check for lack of required documents and for correctly filled in information;
- identification of the Owner and Signatory of the certificate for advanced electronic signature;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Signatory and advances to renewal of the certificate for universal electronic signature.

After the Signatory confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation and submission of an electronic application. All electronic applications for issuance of certificates for advanced electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate.

The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSProvider through its Registration Authority takes measures for the authentication of the private key owner and establishing the fact that this private key is held by the Signatory in accordance with the requested type of certificate for advanced electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSProvider approves the application for renewal of the certificate for advanced electronic signature. The Certification Authority renews the requested *Spektar Org NonUniversal Certificate*.

In case of established lack of correspondence the Signatory is notified by means chosen by him.

Certificates for advanced electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for advanced electronic signature the CSProvider informs the Owner/Signatory that the access to the renewed *Spektar Org NonUniversal Certificate* is open and provides means for this access. The certificate for advanced electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSProvider <http://www.spektar.org>

**The procedure for renewal of the certificate with generation of a new key pair includes the following steps:**

Download from <http://www.spektar.org>, duly fill in and submit to the Registration Authority in person or by mail the following documents:

- Certificate Renewal Application (Form 6) – a copy on paper, signed by the Owner;
- current state certificate, issued within 30 (thirty) days before application date – original or a notarized copy);
- confirmation by the Signatory, certifying his consent to continue to make electronic announcements with all other powers according to the authorization by the Owner (Signatory's Declaration – Form 15).

The documents have to be notarized if they are not submitted in person by the signatories to a representative of the Registration Authority.

The Registration Authority runs a check for authenticity of the information given by the Signatory in a period of up to 5 /five/ days from the date the filled in documents are received.

The check includes:

- check for lack of any of the required documents and for correctly filled in information;
- identification of the Owner and Signatory of the certificate for advanced electronic signature;
- authenticity of the data given.

After establishing the authenticity of the information the Registration Authority notifies the Signatory and advances to renewal of the certificate for universal electronic signature.

After the Signatory confirms his consent with the content of the DN (the information given by him for certification), thus accepting the content of the public part of the *Subject* field of the certificate, he advances to the procedure for generation of a new key pair and an electronic application. All electronic applications for issuance of certificates for advanced electronic signature when the key pair is generated at the Owner/Signatory are signed by the user with the private key which corresponds to the public key in the certificate. The electronic application form is in PKCS#10 format which allows the Registration Authority to check the ownership of the private key.

The CSPProvider through its Registration Authority takes measures for authentication of the private key owner and establishing the fact that this private key is held by the Signatory in accordance with the requested type of certificate for advanced electronic signature.

The measures for identification and establishing the ownership of a private key are described in the *Certification Practice Statement* (Section 3).

In cases of established correspondence the Registration Authority of the CSPProvider approves the application for renewal of the certificate for advanced electronic signature. The Certification Authority renews the requested *Spektar Org NonUniversal Certificate*.

In case of established lack of correspondence the Signatory is notified.

Certificates for advanced electronic signature are not renewed before the user pays for the service.

After the renewal of the certificate for advanced electronic signature the CSPProvider informs the Owner/Signatory that the access to the renewed *Spektar Org NonUniversal Certificate* is open and provides means for this access. The certificate for advanced electronic signature can be accessed via its loading through the web-based interface of the certification services provider CSPProvider <http://www.spektar.org>

#### **4.2.5.7 Certificate revocation**

- revocation of the certificate for advanced electronic signature with expired validity

If there is no application by the Owner or Signatory up to 10 /ten/ days before the expiry date of the certificate for advanced electronic signature, the certificate is revoked automatically on its expiry date.

- revocation of the certificate for advanced electronic signature before its expiry date

The certificate is revoked in cases of termination of the legal person of the certification services provider with no transfer to another certification services provider.

The certification services provider revokes the certificate in case of death or prohibition of the Owner or Signatory; termination of the legal person of the Owner; termination of the representative authority of the Signatory regarding the Owner; establishing that the certificate is issued on the basis of incorrect data.

The certificate is revoked before its expiry date if this is requested by the Owner or Signatory, in person or by mail. Certificate Revocation Application form (Form 10) is needed and it can be downloaded from the internet address <http://www.spektar.org>

In case the application form is not submitted in person it has to be notarized.

After establishing the identity and running additional checks for authenticity of the information given the Registration Authority inputs an electronic application form for status change of the user's certificate. The Certification Authority revokes the certificate by including it in the CRL.