



ISSUANCE AND MANAGEMENT POLICY FOR

Spektar Org NonUniversal Certificate

Revision 2.1

Spektar AD.

11A Carnegie street

1000 Sofia, Bulgaria

phone: + 359 2 9699 200

fax: + 359 2 9699 255

<http://www.spektar.org>

CONTENT

1. Description of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate.....	2
2. Application of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate	3
3. Identification of the issuance and management policy of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate.....	4
4. Profile of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate.....	4
5. Operating rules for issuance and management of the certificate for advanced electronic signature Spektar Org NonUniversal Certificate.....	6
5.1 Application forms	6
5.2. Certificate issuance.....	7
5.3 Certificate publishing	8
5.4 Certificate acceptance by the Owner, Signatory, respectively.....	8
5.5 Suspension and renewal of certificates.....	9
5.5.1 Suspension of the certificate for advanced electronic signature.....	9
5.5.2 Renewal of suspended certificates.....	10
5.6 Certificate renewal.....	10
5.7 Certificate revocation	14

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.

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.

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 Ordinance on the Activities of CSP providers 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. Profile of the certificate for advanced electronic signature *Spektar Org NonUniversal Certificate*

Version	V3	
Serial number	[serial number]	
Signature Algorithm	Sha1RSA	
Issuer	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	
Valid from	[dd Month gggg hh:mm:ss]	
Valid 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 (as well as indication of its nationality)]
	O	Name of organization/trader
	OU	Court or other registration [SR:name of court,D:case type,FD:case number(registration)/yyyy]
	OU	BULSTAT,VAT number (if there is tax number registration) [B:BULSTAT number,DN: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 [BG]
	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]
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 NonUniversal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDist tributionPoint	

	URL= http://www.spektar.org/repository/crl/Spektar NonUniversal 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 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/
Certificate Template Information	Template=SpektarOrgNonUniversal
Enhanced Key Usage	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)
Certificate Policies	Policy Identifier=1.3.6.1.4.1.18463.1.1.2.2.1 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=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
Thumbprint Algorithm	Sha1
Thumbprint	[XXX...]
Issuer Alternate Name	[hyperlink to the registration of the CSProvider in CRC]

*Fields marked * are optional*

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

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 (if there is tax number registration) and BULSTAT.

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.

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>

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).

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.

5.5 Suspension and renewal of certificates

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

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.

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.

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 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 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 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 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>

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>

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.