

***SPEKTAR ORG®***

**ПОЛИТИКА  
ЗА ИЗДАВАНЕ И УПРАВЛЕНИЕ НА  
“Spektar WebServer NonUniversal Certificate”**

**Ревизия 2  
В сила от:**

**Spektar Org®**

**“Спектър” АД**

**ул. “Карнеги” 11А**

**1000 София, България**

**тел.: + 359 2 9699 200**

**факс: + 359 2 9699 255**

**<http://www.spektar.org>**

**СЪДЪРЖАНИЕ**

1. Характеристика на сертификата .....	3
2. Приложение на сертификата .....	3
3. Идентификация на политиката за издаване и управление на сертификат “Spektar WebServer NonUniversal Certificate” .....	4
4. Профил на Spektar WebServer NonUniversal Certificate .....	4
5. Оперативни правила при издаване и управление на „Spektar WebServer NonUniversal Certificate” .....	6
5.1 Заявки за издаване на сертификат .....	6
5.2 Издаване на сертификат .....	7
5.3 Приемане на сертификат от Титуляра, респективно Администратора .....	8
5.4 Публикуване на сертификат .....	9
5.5 Спиране и възобновяване действието на сертификат .....	9
5.5.1 Спиране на сертификат .....	9
5.5.2 Възобновяване на сертификат .....	10
5.6 Подновяване на сертификат .....	11
5.7 Прекратяване на сертификат .....	14

## 1. Характеристика на сертификата

“Spektar WebServer NonUniversal Certificate” се издава на Организация/Търговец Титуляр и Автор- уеб сървър със съответните му идентифициращи характеристики – FQDN(пълно име на сървъра) , като удостоверява връзката им с публичния ключ.

“Spektar WebServer NonUniversal Certificate” има характер на удостоверение за електронен подпис. Всеки електронен подпис, който е придружен от този сертификат има характер на електронен подпис и осигурява увереност по отношение на автентичност, интегритет, конфиденциалност и неотменимост на подписаните съобщения.

Двойката публичен и частен ключове, които кореспондират с издадения сертификат, се генерират и съхраняват на смарт карта, без възможност за извличане на частния ключ от картата.

Издадените сертификати са с валидност 1 /една/ година.

## 2. Приложение на сертификата

“Spektar WebServer NonUniversal Certificate” се използва за сървърни приложения, които изискват най-високо ниво на информационна сигурност, като електронна търговия, финансови трансакции, електронно банкиране, защитен уеб-базиран достъп до конфиденциална информация, екстранет/интранет приложения и други.

При използване на сертификата се осигурява:

- криптирани(защитени) конфиденциални комуникации (SSL или TLS) между уеб сървъра и клиентите (браузър), както и проверка за принадлежността или контрола върху сървъра от съответния Титуляр;
- взаимна автентификация на уеб сървъра с клиентите, изискваща наличие на издадени валидни сертификати на клиентите (браузъра);
- взаимна автентификация и шифроване на комуникации между сървъри с издадени валидни сертификати.

Доставчикът на удостоверителни услуги не носи отговорност за конфигуриране на SSL/TSL частта на уеб сървъра на Титуляра.

Проверка за предназначението и валидността на “Spektar WebServer NonUniversal Certificate” се извършва по следните данни, съдържащи се в профила на сертификата:

- политика, в съответствие на която се издава и управлява сертификатът – посочена в поле “Certificate Policy”;
- предназначението и ограниченията на действието на сертификата – описани в поле “Key Usage”, “Enhanced Key Usage” и “Application Policies”;
- данни за Титуляра и Автора на сертификата – посочени в поле “Subject”.

Доверяващата се страна има задължението да провери предназначението и приложимостта на “Spektar WebServer NonUniversal Certificate“, преди да приеме електронен подпис, придружен от сертификата.

### 3. Идентификация на политиката за издаване и управление на сертификат “Spektar WebServer NonUniversal Certificate”

Политиката за издаване и управление на “Spektar WebServer NonUniversal Certificate” се обозначава с Идентификатор на обекта (OID), който има следната стойност:

<b>OID=</b> 1.3.6.1.4.1.18463.1.1.2.4
---------------------------------------

Съгласно изискванията на НДДУУ политиката за издаване и управление на “Spektar WebServer NonUniversal Certificate” е неразделна част от „Наръчник на потребителя“ и е публикувана на Интернет адрес: <http://www.spektar.org>

### 4. Профил на Spektar WebServer NonUniversal Certificate

<b>Version</b>	V3					
	<b>Serial number</b>	[сериен номер]				
		<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]	
					[dd Month gggg hh:mm:ss]	
CN					<b>Пълно име на Server - FQDN</b>	
T*	<b>Пълно име на Администратора на Server, ЕГН*</b>					
<b>Validit to Subject</b>	O	<b>Наименование на организацията/търговеца</b>				

	OU*	<b>Съдебна или друга регистрация</b> [SR:име на съд,D:вид на дело,FD:номер на дело(регистрация)/гггг]
	OU*	<b>БУЛСТАТ,номер от НДР</b> [B:номер на БУЛСТАТ,DN:номер от НДР(ако има)]
	OU*	<b>Spektar WebServer NonUniversal Certificate</b>
	STREET*	<b>Адрес на управление на Титуляра по удостоверение за актуално състояние или документ за създаване</b> [ул.,номер,бл,вх.,ет.,ап.,град,държава*]
	L	<b>Област по адрес на управление на Титуляра</b> [област]
	PostalCode	<b>Пощенски код по адрес на управление на Титуляра</b>
	S*	<b>Служебен адрес на Администратора съгласно изискванията на чл.24 от ЗЕДЕП</b> [ул.,номер,бл.,вх.,ет.,ап.,град,държава*]
	C	<b>Държава</b> [BG]
	E	<b>Служебен E-mail адрес на Администратора</b>
	Phone	<b>Служебен телефон на Администратора</b> [+35912312341234]
<b>Public Key Type/Length Key Usage (critical)</b>	RSA (1024 Bits)	
	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 Authority Key Identifier</b>	[XXX...]	
	Key ID=[XXX...]	
<b>CRL Distribution Points</b>	Distribution Point Name: Full Name: URL=http://www.spektar.org/repository/crl/Spektar%20NonUniversal%20CA.crl URL=ldap://ldap.spektar.org/O=Spektar%20CA,C=BG,CN=Spektar%20NonUniversal%20CA,CN=Configuration,DC=spektar,DC=org?certificateRevocationList?b	

<b>Authority Information Access</b>	ase?objectClass=cRLDistributionPoint
	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.spektar.org/repository/aia/Spektar%20NonUniversal%20CA.crt Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://ldap.spektar.org/O=Spektar%20CA,C=BG,CN=Spektar%20NonUniversal%20CA,CN=Configuration,DC=spektar,DC=org?cACertificate?base?objectClass=certificationAuthority Authority Info Access 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 Enhanced Key Usage</b>	Template=SpektarWebServerNonUniversal
	Server Authentication (1.3.6.1.5.5.7.3.1) Unknown Key Usage (1.3.6.1.4.1.18463.1.1.2.4)
<b>Certificate Policies</b>	Certificate Policy: Policy Identifier=1.3.6.1.4.1.18463.1.1.2.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.spektar.org/repository/cps
<b>Application Policies</b>	[1]Application Certificate Policy: Policy Identifier=Server Authentication [2]Application Certificate Policy: Policy Identifier=1.3.6.1.4.1.18463.1.1.2.4
<b>Thumbprint Algorithm</b>	Sha1
<b>Thumbprint Issuer Alternate Name</b>	[XXX...] [хиперлинк към регистрацията на Доставчика в КРС]

Полетата маркирани с "\*" са опционални.

## 5. Оперативни правила при издаване и управление на „Spektar WebServer NonUniversal Certificate“

### 5.1 Заявки за издаване на сертификат

Лицето, желаещо да му бъде издаден сертификат "Spektar WebServer NonUniversal Certificate", наричано по-долу за краткост Заявител, надлежно попълва и предоставя на Регистриращия орган лично или по пощата следните документи:

- заявка за издаване на сертификат (Бланка Образец2.6);
- договор за удостоверявателни услуги (2 екземпляра);
- заявка за удостоверявателни услуги (Бланка Образец3).

Документи, идентифициращи Титуляра - Организация/Търговец:

- данни за Организация/Търговец (Бланка Образец4.1);
- фирмено решение или друг документ, удостоверяващи възникването- оригинал и нотариално заверено копие;
- удостоверение за актуално състояние, издадено в рамките на 30(тридесет) дни преди датата на подаване на заявката- оригинал или нотариално заверено копие;
- копие от НДР и БУЛСТАТ.

Документи, идентифициращи Администратора на сървъра:

- нотариално заверено пълномощно (Бланка Образец13), с което Титулярът овластява Администратора;
- саморъчно подписано копие от личната карта на Администратора;
- декларация на Администратора (Бланка Образец15).

Заявителят може да изтегли посочените образци на документи от Интернет адрес:

<http://www.spektar.org>

В случай, че документите не се предават лично на представител на Регистриращия орган, се изисква нотариална заверка.

Регистриращият орган извършва проверка за достоверност на подадената информация от Заявителя в срок до 5 /пет/ работни дни от датата на получаване на попълнените документи. Проверката включва:

- проверка за липса на изисквани документи и коректност на попълването на документите;
- идентификация на Титуляра и Администратора на сертификата;
- достоверност на попълнените данни.

В случай на отказ за издаване на сертификат, Регистриращият орган уведомява Заявителя и посочва причината за отхвърляне на заявката.

Посредством уеб- базиран интерфейс Администраторът има възможност да проследява и управлява процесите по издаване и управление на сертификата.

## 5.2 Издаване на сертификат

След като Администраторът е потвърдил съгласието си със съдържанието на DN(предоставената от него информация за удостоверяване), той пристъпва към процедурата по генериране на двойката частен-публичен ключове и подаване на

електронна заявка. Всички електронни заявки за издаване на сертификати, когато двойката ключове се генерира при Титуляра/Администратора, са подписани от потребителя с частния ключ, който кореспондира с публичния ключ в заявката. Електронната заявка е в PKCS#10 формат, което позволява на Регистриращият орган на Spektar Org® да се увери, че Администраторът държи частния ключ.

Spektar Org®, чрез Регистриращия си орган, реализира мерки за автентификация на притежателя на частния ключ и установяване на факта, че този частен ключ се държи от Администратора, в съответствие със заявения тип сертификат.

Мерките за идентификация и установяване притежаването на частен ключ са описани в „Практика при предоставяне на удостоверителни услуги на Spektar Org“(Секция 3).

При констатирано съответствие Регистриращият орган на Spektar Org® одобрява заявката за сертификат. Удостоверяващият орган потвърждава и издава “Spektar WebServer NonUniversal Certificate” .

При констатирано несъответствие се уведомява потребителя.

Сертификатът не се издава преди потребителят да извърши заплащане на услугата.

След генерирането на сертификат, Spektar Org® уведомява Титуляра/Администратора, че достъпът до заявения “Spektar WebServer NonUniversal Certificate” е осигурен и предоставя начин за получаването му. Достъпът до сертификата може да бъде осъществен чрез зареждането му през сайта на доставчика на удостоверителни услуги Spektar Org® <http://www.spektar.org>

### **5.3 Приемане на сертификат от Титуляра, респективно Администратора**

Титулярът или Администраторът могат в 3 /три/ дневен срок след зареждане и инсталиране на сертификата да направят рекламация за коректността на съдържанието му.

Ако след изтичане на този срок Титулярът/Администраторът не е направил рекламации относно коректността на съдържанието, сертификатът се счита за окончателно приет.

Сертификатът се счита за окончателно приет от Титуляра и Администратора, ако преди изтичане на 3 /три/ дневния срок след издаването му бъде използван поне веднъж.

#### 5.4 Публикуване на сертификат

Издаденият от Удостоверяващия орган на Spektar Org® сертификат се публикува веднага след генерирането му в електронния регистър на доставчика.

Електронният регистър на Spektar Org® е публичен и начините за достъп до него са описани в “Практика при предоставяне на удостоверителни услуги на Spektar Org” (Секция 2.3).

#### 5.5 Спиране и възобновяване действието на сертификат

##### 5.5.1 Спиране на сертификат

Спиране на действието на издадени от Spektar Org® сертификати се предприема при наличие на определени основания, като срокът за който е спряно действието на сертификат зависи от обстоятелствата довели до спиране. Този срок не може да надвишава 48 часа.

Искане за спиране на сертификат може да бъде отправено до Spektar Org® по някой от следните начини:

- на телефонни номера +359 2 9699200/ 252

лицето, което иска спирането, трябва да съобщи:

трите си имена;

телефонният номер, от който се обажда за спиране на сертификат; /този телефонен номер се използва за обратна контрола/

сериен номер на сертификата, който желае да бъде спряно;

причините, поради които иска спиране на съответния сертификат.

Когато Титулярът/Администраторът е поискал спиране, се изисква да съобщи и паролата за идентификация, която е попълнил в заявката за сертификат.

- електронна поща

лицето, което иска спиране, изтегля от Интернет сайта на Spektar Org® „Заявка за спиране на действието на сертификат“ (Бланка Образец8);

попълва изтеглената форма (Бланка Образец8) и я изпраща като прикачен файл в електронна поща на адрес: [info@spektar.org](mailto:info@spektar.org)

Когато лицето е Титуляра/Администратора, съобщава и паролата за идентификация, която е попълнил в заявката за сертификат.

- през Интернет сайта на Spektar Org®

заявителят попълва и изпраща електронна форма „Заявка за спиране на действието на сертификат“ (Бланка Образец8).

- лично при доставчика на Удостоверителни услуги лицето, което иска спиране, лично при Доставчика на Удостоверителни услуги Spektar Org® попълва „Заявка за спиране на действието на сертификат“ (Бланка Образец8).

Spektar Org® спира действието на сертификата като го поставя в списъка с прекратени сертификати със статус „HOLD“.

Spektar Org® идентифицира, но не удостоверява самоличността на лицето, поискало спиране на сертификата.

Spektar Org® незабавно уведомява Титуляра и Администратора за спирането на сертификата.

#### **5.5.2 Възобновяване на сертификат**

Спрян сертификат се възобновява, ако в рамките на законово регламентирания максимално допустим 48-часов срок Титулярът предостави надлежно попълнена и подписана „Заявка за възобновяване на сертификат за електронен подпис“ (Бланка Образец9).

„Заявка за възобновяване на сертификат за електронен подпис“ (Бланка Образец9) се попълва от Титуляра при отпадане на основанието за спиране, и с която уверява Доставчика на удостоверителни услуги, че е узнал причината за спирането, както и че искането за възобновяване е направено вследствие на узнаването.

В случаите, когато искането за спиране произхожда от Комисията за регулиране на съобщенията, Spektar Org® предоставя на комисията копие от писмената заявка за възобновяване.

Възобновяването се извършва чрез изваждането на сертификата със статус “HOLD” от списъка с прекратени сертификати (CRL) в електронния регистър на Spektar Org®.

Ако след изтичане на максимално регламентираният 48 /четиридесет и осем/ часов срок от спиране на сертификата не е налице основание за неговото прекратяване, Spektar Org® автоматично възобновява сертификата.

## 5.6 Подновяване на сертификат

Сертификати на Титуляри, които не са прекратени, могат да бъдат подновени преди изтичане на срока им на валидност, без да е необходимо генериране на нова двойка ключове.

Spektar Org® като доставчик на удостоверителни услуги допуска подновяване на сертификат чрез използване на съществуващата двойка ключове еднократно, с цел да се намали риска от компрометирането ѝ.

В „Практика за предоставяне на удостоверителни услуги на Spektar Org“ (Секция 4 ) има подробно описание на методите за подновяване на сертификата и съображения за сигурност, които да бъдат отчетени при конкретния избор на Администратора.

### **Процедурата по продължаване действието на сертификат без да се генерира нова двойка ключове включва следните стъпки:**

Администраторът изтегля от Интернет адрес: <http://www.spektar.org>, надлежно попълва и предава на Регистриращия орган лично или по пощата следните документи:

- заявка за подновяване на сертификат за електронен подпис (Бланка Образец6) – хартиено копие;
- удостоверение за актуално състояние, издадено в рамките на 30(тридесет) дни преди датата на подаване на заявката- оригинал или нотариално заверено копие;
- потвърждение от Администратора, удостоверяващо съгласието му да продължи да прави електронни изявления и с всички други правомощия, съгласно упълномощаването му от Титуляра (Декларация от Администратора- Бланка Образец15).

В случай, че документите не се предават лично на представител на Регистриращия орган, се изисква нотариална заверка.

Регистриращият орган извършва проверка за достоверност на подадената информация от Администратора в срок до 5 /пет/ работни дни от датата на получаване на попълнените документи. Проверката включва:

- проверка за липса на изисквани документи и коректност на попълването на документите;
- идентификация на Титуляра и Администратора на сертификата;
- достоверност на попълнените данни.

След установяване на достоверност на информацията, Регистриращият орган

уведомява Администратора и пристъпва към подновяване на сертификата.

След като Администраторът е потвърдил съгласието си със съдържанието на DN(предоставената от него информация за удостоверяване), той пристъпва към процедурата по генериране и подаване на електронна заявка. Всички електронни заявки за издаване на сертификати, когато двойката ключове се генерира при Титуляра/Администратора, са подписани от потребителя с частния ключ, който кореспондира с публичния ключ в заявката. Електронната заявка е в PKCS#10 формат, което позволява на Регистриращият орган на Spektar Org® да провери притежанието на частния ключ.

Spektar Org®, чрез Регистриращия си орган, реализира мерки за автентификация на притежателя на частния ключ и установяване на факта, че този частен ключ се държи от Администратора, в съответствие със заявления тип сертификат.

Мерките за идентификация и установяване притежаването на частен ключ са описани в „Практика при предоставяне на удостоверителни услуги на Spektar Org“(Секция 3).

При констатирано съответствие Регистриращият орган на Spektar Org® одобрява заявката за подновяване на сертификата. Удостоверяващият орган подновява заявления „Spektar WebServer NonUniversal Certificate“ .

При констатирано несъответствие се уведомява Администратора.

Сертификатът не се подновява преди потребителят да извърши заплащане на услугата.

След подновяването на сертификата, Spektar Org® уведомява Титуляра/Администратора, че достъпът до подновения „Spektar WebServer NonUniversal Certificate“ е осигурен и предоставя начин за получаването му. Достъпът до сертификата може да бъде осъществен чрез зареждането му през уеб-базирания интерфейс на доставчика на удостоверителни услуги Spektar Org® <http://www.spektar.org>

**Процедурата по продължаване действието на сертификат с генериране на нова двойка ключове включва следните стъпки:**

Администраторът изтегля, надлежно попълва и предава на Регистриращия орган лично или по пощата следните документи:

- заявка за подновяване на сертификат за електронен подпис (Бланка Образец6) – хартиено копие.

- потвърждение от Администратора, удостоверяващо съгласието му да продължи да прави електронни изявления и с всички други правомощия, съгласно упълномощаването му от Титуляра (Декларация от Администратора- Бланка Образец15).

Изисква се когато Титулярът и Администраторът са различни лица.

В случай, че документите не се предават лично на представител на Регистриращия орган, се изисква нотариална заверка.

Регистриращият орган извършва проверка за достоверност на подадената информация от Администратора в срок до 5 /пет/ работни дни от датата на получаване на попълнените документи. Проверката включва:

- проверка за липса на изисквани документи и коректност на попълването на документите;
- идентификация на Титуляра и Администратора на сертификата;
- достоверност на попълнените данни.

След установяване на достоверност на информацията, Регистриращият орган уведомява Администратора и пристъпва към подновяване на сертификата.

След като потребителят е потвърдил съгласието си със съдържанието на DN(предоставената от него информация за удостоверяване), той пристъпва към процедурата по генериране на нова двойка частен-публичен ключове и на електронна заявка. Всички електронни заявки за издаване на сертификати, когато двойката ключове се генерира при Титуляра/Администратора, са подписани от потребителя с частния ключ, който кореспондира с публичния ключ в заявката. Електронната заявка е в PKCS#10 формат, което позволява на Регистриращият орган на Spektar Org® да провери притежанието на частния ключ.

Spektar Org®, чрез Регистриращия си орган, реализира мерки за автентификация на притежателя на частния ключ и установяване на факта, че този частен ключ се държи, в съответствие със заявления тип сертификат.

Мерките за идентификация и установяване притежаването на частен ключ са описани в „Практика при предоставяне на удостоверителни услуги на Spektar Org“(Секция 3).

При констатирано съответствие Регистриращият орган на Spektar Org® одобрява заявката за подновяване на сертификата. Удостоверяващият орган подновява заявеният “Spektar WebServer NonUniversal Certificate” .

При констатирано несъответствие се уведомява потребителя.

Сертификатът не се подновява преди потребителят да извърши заплащане на услугата.

След подновяването на сертификата, Spektar Org® уведомява Титуляра/Администратора, че достъпът до подновения “Spektar WebServer NonUniversal Certificate” е осигурен и предоставя начин за получаването му. Достъпът до сертификата може да бъде осъществен чрез зареждането му през уеб-базирания интерфейс на доставчика на удостоверителни услуги Spektar Org® <http://www.spektar.org>

### 5.7 Прекратяване на сертификат

- прекратяване действието на сертификат с изтичане срока на валидност

При неподadena заявка за подновяване от страна на Титуляра или Администратора до 10 /десет/ дни преди изтичане на срока на действието на сертификата, действието на сертификата се прекратява автоматично, с изтичане срокът му на валидност.

- прекратяване действието на сертификат преди изтичане срока на валидност

Сертификатът може да бъде предсрочно прекратен при изразено желание от страна на Титуляра или Администратора, заявено лично или по пощата.

Необходимо е представяне на заявка за прекратяване на сертификат(Бланка Образец10), която може да бъде изтеглена от Интернет адрес <http://www.spektar.org>

В случай, че заявката не се предава лично на представител на Регистриращия орган, се изисква нотариална заверка.

След като се увери в самоличността и представителната власт на Титуляра/Администратора, и извърши допълнителна проверка за достоверност на подадената информация, Регистриращият орган въвежда електронна заявка за промяна в статуса на сертификата на потребителя. Удостоверяващият орган реализира прекратяването като включва сертификата в CRL.