

SPEKTAR ORG®

**ПОЛИТИКА
ЗА ИЗДАВАНЕ И УПРАВЛЕНИЕ НА
“Spektar Object 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 Object NonUniversal Certificate" | 4 |
| 4. Профил на Spektar Object NonUniversal Certificate | 4 |
| 5. Оперативни правила при издаване и управление на „Spektar Object 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 Автора | 8 |
| 5.4 Публикуване на сертификат | 8 |
| 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 | 10 |
| 5.7 Прекратяване на сертификат | 14 |

1. Характеристика на сертификата

“Spektar Object NonUniversal Certificate” се издава на Титуляр Организация/Търговец и Автор физическо лице, като удостоверява тяхната самоличност и връзката им с публичния ключ.

“Spektar Object 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.

“Spektar Object NonUniversal Certificate” се използва за подписване и разпространение на софтуер- файлове с данни, файлове с изпълним код, файлове с програмен код, файлове с музика, графика, видеоклипове и др.

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

Сертификатът и кореспондиращата с него двойка частен и публичен ключове има следните приложения:

- поставяне на електронен подпис (Digital Signature) – за доказване на цялостта на данните в подписания електронен документ, предпазване на документа от последващи промени и показване на връзката между документа и Автора;
- доказване на факта на изявлението (Non-Repudiation) – за установяване на самоличността на Автора на електронния подпис;
- шифриране на ключове (Key encipherment) – при размяна на ключове използвани за шифриране на данни;
- шифриране на данни (Data encipherment) – при предаване на данни през незащитена комуникационна среда или при архивиране.

„Spektar Object Universal Certificate” може да бъде използван за идентифициране на Титуляра и Автора при използване на персонална електронна поща, достъп до защитени информационни системи и електронна търговия. С кореспондиращата двойка ключове

може да се поставя електронен подпис и да се криптират данни.

Проверка за предназначението и валидността на “Spektar Object 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 Object NonUniversal Certificate”, преди да приеме електронен подпис, придружен от сертификата.

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

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

| |
|---------------------------------------|
| OID= 1.3.6.1.4.1.18463.1.1.2.5 |
|---------------------------------------|

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

4. Профил на Spektar Object NonUniversal Certificate

| | | |
|----------------------------|--------------------------|--|
| Version | V3 | |
| Serial number | [сериен номер] | |
| 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] | |
| | [dd Month gggg hh:mm:ss] | |
| Validit to | [dd Month gggg hh:mm:ss] | |

| | | |
|--|--|--|
| Subject | CN | Пълно име на Автора,овластен да подписва софтуерен обект |
| | T | Основание за представителна власт на Автора [длъжност,N:номер на нотариус.номер на документ/дд/мм/гггг,EGN*:ЕГН] |
| | O | Наименование на организацията/търговеца |
| | OU | Съдебна или друга регистрация [SR:име на съд,D:вид на дело,FD:номер на дело(регистрация)/гггг] |
| | OU | БУЛСТАТ,номер от НДР [B:номер на БУЛСТАТ,DN:номер от НДР(ако има)] |
| | OU | Spektar Object NonUniversal Certificate |
| | STREET | Адрес на управление на Титуляра по удостоверение за актуално състояние/съдебна или друга регистрация [ул.,номер,бл,вх.,ет.,ап.,град,държава*] |
| | L | Област по адрес на управление на Титуляра [област] |
| | PostalCode | Пощенски код по адрес на управление на Титуляра |
| | S | Служебен адрес на Автора [ул.,номер,бл.,вх.,ет.,ап.,град,държава*] |
| | C | Държава [BG] |
| | E | Е-mail адрес на Автора, за който се издава сертификата |
| | Phone | Служебен телефон на Автора [+35912312341234] |
| Public Key Type/Length Key Usage (critical) | RSA (1024 Bits) | |
| | 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 KeyIdentifier Authority Key Identifier CRL Distribution Points | [XXX...] |
| | Key ID=[XXX...] |
| | URL=ldap:///CN=Spektar NonUniversal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDistributi onPoint 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=SpektarObjectNonUniversal |
| Enhanced Key Usage | Document Signing (1.3.6.1.4.1.311.10.3.12) SpektarObjectNonUniversalPolicy (1.3.6.1.4.1.18463.1.1.2.5) 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=1.3.6.1.4.1.18463.1.1.2.5.1 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=SpektarObjectNonUniversalPolicy(1.3.6.1.4.1.18463.1.1.2.5) [3]Application Certificate Policy: Policy Identifier=Client Authentication [4]Application Certificate Policy: Policy Identifier=Secure Email |
| Thumbprint Algorithm Thumbprint Issuer Alternate Name | Sha1 |
| | [XXX...] |
| | [хиперлинк към регистрацията на Доставчика в КРС] |

Полетата маркирани с "" са опционални.*

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

5.1 Заявки за издаване на сертификат

Лицето, желаещо да му бъде издаден сертификат „Spektar Object NonUniversal Certificate“, наричано по-долу за краткост Заявител, надлежно попълва и предоставя на

Регистриращия орган лично или по поща следните документи:

- заявка за издаване на сертификат (Бланка Образец 2.5);
- договор за удостоверявателни услуги (2 екземпляра);
- заявка за удостоверявателни услуги (Бланка Образец 3).

Документи, идентифициращи Титуляра - Организация/Търговец:

- нотариално заверено пълномощно (Бланка Образец 13), с което Титулярът овластява Автора;
- саморъчно подписано копие от личната карта на Автора;
- декларация на Автора (Бланка Образец 15).

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 на всички документи.

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 Автора 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 веб- базиран интерфейс Авторът има възможност да проследява и управлява процесите по издаване и управление на сертификата.

5.2 Издаване на сертификат

След като Авторът 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/Автора, 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 Авторът 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 Автора, 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 Object 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/Автора, че достъпът до заявения „*Spektar Object 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 Автора

Титулярът или Авторът 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/Авторът не е направил рекламации относно коректността на съдържанието, сертификатът се счита за окончателно приет.

Сертификатът се счита за окончателно приет от Титуляра и Автора, 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/Авторът 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 Образец 8);
попълва изтеглената форма Бланка Образец 8 и я изпраща като прикачен файл в електронна поща на адрес: info@spektar.org

Когато лицето е Титуляра/Автора, 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 Образец 8).
- 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 Образец 8).

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 Автора за спирането на сертификата.

5.5.2 Възобновяване на сертификат

Срян 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-образец 9).

„Заявка за възобновяване на сертификат за електронен подпис“ (Бланка Образец 9) 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 Автора.

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

Авторът 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-образец 6) – 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 Автора, удостоверяващо съгласието му да продължи да прави електронни изявления и с всички други правомощия, съгласно упълномощаването му от Титуляра (Декларация от Автора- Бланка-образец 15).

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 Автора 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 Автора на сертификата;
- достоверност на попълнените данни.

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

След като Авторът 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/Автора, 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 Автора, 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 подновяване на сертификата. Удостоверяващият орган подновява заявеният „Spektar Object NonUniversal Certificate“ .

При констатирано несъответствие се уведомява Автора.

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

След подновяването на сертификата, Spektar Org® уведомява Титуляра/Автора, че достъпът до подновения „Spektar Object 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:

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

- заявка за подновяване на сертификат за електронен подпис (Бланка-образец 6) – хартиено копие;
- потвърждение от Автора, удостоверяващо съгласието му да продължи да прави електронни изявления и с всички други правомощия, съгласно упълномощаването му от Титуляра (Декларация от Автора- Бланка-образец 15);

Изисква се когато Титулярът и Авторът 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 Автора 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 Автора на сертификата;
- достоверност на попълнените данни.

След установяване на достоверност на информацията, Регистриращият орган уведомява Автора 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/Автора, 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 Object 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/Автора, че достъпът до подновения „Spektar Object 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 неподадена заявка за подновяване от страна на Титуляра или Автора 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 Автора, заявено лично или по пощата.

Необходимо е представяне на заявка за прекратяване на сертификат(Бланка-образец 10), 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/Автора, 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.