



ПОЛИТИКА ЗА ИЗДАВАНЕ И УПРАВЛЕНИЕ НА “Spektar Personal NonUniversal Certificate”

Ревизия 2.1

“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 удостоверение за усъвършенстван електронен подпис “Spektar Personal NonUniversal Certificate”	2
2. Приложение на удостоверение за усъвършенстван електронен подпис “Spektar Personal NonUniversal Certificate”	3
3. Идентификация на политиката за издаване и управление на удостоверение за усъвършенстван електронен подпис “Spektar Personal NonUniversal Certificate”	4
4. Профил на удостоверение за усъвършенстван електронен подпис “Spektar Personal NonUniversal Certificate”	4
5. Оперативни правила при издаване и управление на удостоверение за усъвършенстван електронен подпис “Spektar Personal NonUniversal Certificate”	6
5.1 Заявки за издаване на удостоверението.....	6
5.2 Издаване на удостоверението	7
5.3 Публикуване на удостоверението.....	8
5.4 Приемане на удостоверението от Титуляра, респективно Автора.....	8
5.5 Спиране и възобновяване действието на удостоверението	8
5.5.1 Спиране на удостоверение	8
5.5.2 Възобновяване на удостоверението.....	10
5.6 Подновяване на удостоверението	10
5.7 Прекратяване на удостоверението	13

1. Характеристика на удостоверение за усъвършенстван електронен подпис “Spektar Personal NonUniversal Certificate”

“Spektar Personal NonUniversal Certificate” се издава на физически лица Титуляр и Автор, като удостоверява тяхната самоличност и връзката им с публичния ключ.

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

Двойката частен-публичен ключ, които кореспондират с издаденото удостоверение, се генерират и съхраняват на смарт карта, без възможност за извличане на частния ключ от картата.

Издадените удостоверения са с валидност 1 /една/ година.

2. Приложение на удостоверение за усъвършенстван електронен подпис “Spektar Personal NonUniversal Certificate”

Удостоверението за усъвършенстван електронен подпис и кореспондиращата с него двойка частен-публичен ключ 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 Personal NonUniversal Certificate” може да бъде използван за идентифициране на Титуляра/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 шифрират данни.

Проверка за предназначението и валидността на “Spektar Personal NonUniversal Certificate” се извършва по следните данни, съдържащи се в профила на удостоверението за усъвършенстван електронен подпис:

- политика, в съответствие на която се издава и управлява удостоверение за усъвършенстван електронен подпис – посочена в поле “Certificate Policy”;
- предназначението и ограниченията на действието на удостоверението за усъвършенстван електронен подпис – описани в поле “Key Usage”, “Enhanced Key Usage” и “Application Policies”;

- данни за Титуляра/Автора на удостоверението за усъвършенстван електронен подпис – посочени в поле “Subject”.

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

3. Идентификация на политиката за издаване и управление на удостоверение за усъвършенстван електронен подпис “Spektar Personal NonUniversal Certificate”

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

OID=1.3.6.1.4.1.18463.1.1.2.1

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

4. Профил на удостоверение за усъвършенстван електронен подпис “Spektar Personal 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]	
Validit to	[dd Month gggg hh:mm:ss]	

Subject	CN	Пълно име на Автора
	O	Пълно име на Титуляра [NT:име]
	OU*	ЕГН на Титуляра* [EGNT:ЕГН или ЛНЧ или дата на раждане (ггммдд)]
	OU	Spektar Personal NonUniversal Certificate
	STREET	Адрес на Титуляра за кореспонденция [ул.,номер,бл,вх.,ет.,ап.,град,държава*]
	L	Област по адрес на Титуляра [област]
	PostalCode	Пощенски код по адрес по лична карта на Титуляра
	S	Постоянен адрес на Автора [ул.,номер,бл.,вх.,ет.,ап.,град,държава*]
	C	Държава [XX]
	E	Е-mail адрес на Автора, за който се издава удостоверение за усъвършенстван електронен подпис
	Phone	Телефон на Автора [+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 NonUniversal CA,CN=CDP, DC=spektar,DC=org?certificateRevocationList?base?objectClass=cRLDist ributionPoint 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=certificationAu thority 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=SpektarPersonalNonUniversal
Enhanced Key Usage	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)
Certificate Policies	Policy Identifier=1.3.6.1.4.1.18463.1.1.2.1.1 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=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
Thumbprint Algorithm	Sha1
Thumbprint	[XXX...]
Issuer Alternate Name	[хиперлинк към регистрацията на Доставчика в КРС]

Полетата маркирани с "*" са опционални.

5. Оперативни правила при издаване и управление на удостоверение за усъвършенстван електронен подпис "Spektar Personal NonUniversal Certificate"

5.1 Заявки за издаване на удостоверението

Лицето, желаещо да му бъде издадено удостоверение за усъвършенстван електронен подпис "Spektar Personal 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 удостоверение за усъвършенстван електронен подпис (Бланка Образец2.9);
- договор за удостоверителни услуги (2 екземпляра);
- заявка за удостоверителни услуги (Бланка Образец3).
- данни за Титуляра физическо лице (Бланка Образец4.2);
- саморъчно подписано копие от личната карта на Титуляра и изписан текст **„Съгласен съм да се ползва копието на личната ми карта за целите на ДУУ ”**.

Съгласието се изисква във връзка със Закона за защита на личните данни.

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 подписите.

След подписването му и от страна на ДУУ, екземпляр от договора за удостоверявателни услуги се изпраща на Заявителя по поща, с обратна разписка, на посочен от него адрес за контакт.

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/Автора на удостоверението;
- достоверност на попълнените данни.

В случай на отказ за издаване на удостоверение за усъвършенстван електронен подпис, Регистриращият орган уведомява Заявителя чрез избран от посочените от него начини за комуникация и посочва причината за отхвърляне на заявката.

Посредством веб- базиран интерфейс Авторът има възможност да проследява и управлява процесите по издаване и управление на удостоверението за усъвършенстван електронен подпис.

5.2 Издаване на удостоверението

След като Авторът е потвърдил съгласието си със съдържанието на DN(предоставената от него информация за удостоверяване), като по този начин приема съдържанието на публичната част от полето “Subject” от удостоверението, той пристъпва към процедурата по генериране на двойката частен-публичен ключ и подаване на електронна заявка. Всички електронни заявки за издаване на удостоверения за усъвършенстван електронен подпис, 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 Регистриращия орган на ДУУ да се увери, че Авторът държи частния ключ.

ДУУ, 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 заявления тип удостоверение за усъвършенстван електронен подпис.

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

При констатирано съответствие Регистриращият орган на ДУУ одобрява заявката за удостоверение за усъвършенстван електронен подпис. Удостоверяващият орган потвърждава и

издава “Spektar Personal NonUniversal Certificate” .

При констатирано несъответствие се уведомява Заявителя по избран подходящ начин, предоставен от него за контакт.

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

След издаване на удостоверението ДУУ уведомява Титуляра/Автора и му предоставя начин за получаване. Достъпът до удостоверението за усъвършенстван електронен подпис може да бъде осъществен чрез зареждането му през сайта на ДУУ <http://www.spektar.org> .

5.3 Публикуване на удостоверението

Издаденото от Удостоверяващия орган на ДУУ удостоверение за усъвършенстван електронен подпис се публикува веднага след генерирането му в електронния регистър на доставчика.

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

5.4 Приемане на удостоверението от Титуляра, респективно Автора

Титулярът или Авторът могат в 3 /три/ дневен срок след зареждане и инсталиране на удостоверението за усъвършенстван електронен подписа да направят рекламация за коректността на съдържанието му.

Ако след изтичане на този срок Титулярът/Авторът не е направил рекламации относно коректността на съдържанието, удостоверението се счита за окончателно прието.

Удостоверението за усъвършенстван електронен подпис се счита за окончателно прието от Титуляра/Автора, ако преди изтичане на 3 /три/ дневния срок след издаването му бъде използвано поне веднъж.

5.5 Спиране и възобновяване действието на удостоверението

5.5.1 Спиране на удостоверение

Спиране на действието на издадени от ДУУ удостоверения за усъвършенстван електронен подпис се предприема при наличие на определени основания, като срокът за който е спряно действието на удостоверението зависи от обстоятелствата довели до спиране. Този срок не може да надвишава 48 часа от момента на спирането.

Искане за спиране на удостоверение за усъвършенстван електронен подпис може да бъде отправено до ДУУ 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 удостоверение за усъвършенстван електронен подпис; /този телефонен номер се използва за обратна контрола/;

сериен номер на удостоверението за усъвършенстван електронен подпис, който желае да бъде спряно;

причините, поради които иска спиране на съответното удостоверение.

Когато Титулярът/Авторът е поискал спиране, се изисква да съобщи и паролата за идентификация, която е попълнил в заявката за удостоверение за усъвършенстван електронен подпис.

- електронна поща

лицето, което иска спиране, изтегля от Интернет сайта на ДУУ „Заявка за спиране на действието на удостоверение за усъвършенстван електронен подпис“ (Бланка Образец8);

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

Когато лицето е Титуляра/Автора, съобщава и паролата за идентификация, която е попълнил в заявката за удостоверение за усъвършенстван електронен подпис.

- през Интернет сайта на ДУУ

заявителят попълва и изпраща електронна форма „Заявка за спиране на действието на удостоверение за усъвършенстван електронен подпис“ (Бланка Образец8).

- лично при доставчика на Удостоверителни услуги

лицето, което иска спиране лично при Доставчика на Удостоверителни услуги ДУУ, попълва „Заявка за спиране на действието на удостоверение за усъвършенстван електронен подпис“ (Бланка Образец8).

ДУУ спира действието на удостоверение за усъвършенстван електронен подпис като го поставя в списъка с прекратени удостоверения със статус „HOLD“.

ДУУ идентифицира, но не удостоверява самоличността на лицето, поискало спиране на

удостоверение.

ДУУ незабавно уведомява Титуляра/Автора за спирането на удостоверението.

5.5.2 Възобновяване на удостоверението

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

„Заявка за възобновяване на удостоверение за усъвършенстван 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, ДУУ предоставя на комисията копие от писмената заявка за възобновяване.

Възобновяването се извършва чрез изваждането на удостоверението със статус “HOLD” от списъка с прекратени удостоверения (CRL) в електронния регистър на ДУУ.

Ако след изтичане на максимално регламентираният 48 /четиридесет и осем/ часов срок от спиране на удостоверение не е налице основание за неговото прекратяване, ДУУ автоматично възобновява удостоверението.

5.6 Подновяване на удостоверението

Удостоверения за усъвършенстван електронен подпис, които не са прекратени, могат да бъдат подновени преди изтичане на срока им на валидност, без да е необходимо генериране на нова двойка ключове.

ДУУ като доставчик на удостоверителни услуги допуска подновяване на удостоверение за усъвършенстван електронен подпис чрез използване на съществуващата двойка ключове еднократно, с цел да се намали риска от компрометирането ѝ.

В „Практика за предоставяне на удостоверителни услуги“ (Секция 4) има подробно описание на методите за подновяване на удостоверението за усъвършенстван електронен подпис и съображения за сигурност, които да бъдат отчетени при конкретния избор на Автора.

Процедурата по подновяване действието на удостоверение, без да се генерира нова двойка ключове включва следните стъпки:

Изтегляне от Интернет адрес: <http://www.spektar.org>, надлежно попълване и предаване на Регистриращия орган лично или по пощата на заявка за подновяване на удостоверение (Бланка Образецб) – хартиено копие, подписано от Титуляра;

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

Регистриращият орган извършва проверка за достоверност на подадената информация от Титуляра/Автора в срок до 5 /пет/ работни дни от датата на получаване на надлежно попълнения документ. Проверката включва:

- проверка за коректност по съдържанието на предоставената заявка;
- идентификация на Титуляра/Автора на удостоверението;
- достоверност на попълнените данни.

След установяване на достоверност на информацията, Регистриращият орган уведомява Титуляра/Автора и пристъпва към подновяване на удостоверението.

След като Титулярът/Авторът е потвърдил съгласието си със съдържанието на DN(предоставената от него информация за удостоверяване), като по този начин приема съдържанието на публичната част от полето “Subject” от удостоверението, той пристъпва към процедурата по генериране и подаване на електронна заявка. Всички електронни заявки за подновяване на удостоверения за усъвършенстван електронен подпис, 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 ДУУ да провери притежанието на частния ключ.

ДУУ, 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 удостоверение.

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

При констатирано съответствие Регистриращият орган на ДУУ одобрява заявката за подновяване на удостоверението. Удостоверяващият орган подновява заявеният “Spektar

Personal NonUniversal Certificate” .

При констатирано несъответствие се уведомява Автора, по избран подходящ начин, предоставен от него за контакт.

Удостоверение за усъвършенстван електронен подпис не се подновява преди потребителят да извърши заплащане на услугата.

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

Процедурата по подновяване действието на удостоверение с генериране на нова двойка ключове включва следните стъпки:

Изтегляне от Интернет адрес: <http://www.spektar.org>, надлежно попълване и предаване на Регистрирания орган лично или по пощата на заявка за подновяване на удостоверение (Бланка Образецб) – хартиено копие, подписано от Титуляра;

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

Регистрираният орган извършва проверка за достоверност на подадената информация от Титуляра/Автора в срок до 5 /пет/ работни дни от датата на получаване на надлежно попълнения документ. Проверката включва:

- проверка за коректност по съдържанието на предоставената заявка;
- идентификация на Титуляра/Автора на удостоверението;
- достоверност на попълнените данни.

След установяване на достоверност на информацията, Регистрираният орган уведомява Титуляра/Автора и пристъпва към подновяване на удостоверението.

След като потребителят е потвърдил съгласието си със съдържанието на DN(предоставената от него информация за удостоверяване), като по този начин приема съдържанието на публичната част от полето “Subject” от удостоверението, той пристъпва към процедурата по генериране на нова двойка частен-публичен ключ и на електронна заявка. Всички електронни заявки за подновяване на удостоверения за усъвършенстван електронен подпис, 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 ДУУ да провери притежанието на частния ключ.

ДУУ, 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 заявения тип удостоверение за усъвършенстван електронен подпис.

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

При констатирано съответствие Регистриращият орган на ДУУ одобрява заявката за подновяване на удостоверение за усъвършенстван електронен подпис. Удостоверяващият орган подновява заявеният “Spektar Personal NonUniversal Certificate” .

При констатирано несъответствие се уведомява Автора, по избран подходящ начин, предоставен от него за контакт.

Удостоверение за усъвършенстван електронен подпис не се подновява преди потребителят да извърши заплащане на услугата.

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

5.7 Прекратяване на удостоверението

- прекратяване действието на удостоверение за усъвършенстван електронен подпис с изтичане срока на валидност

При неподадена заявка за подновяване от страна на Титуляра/Автора до 10 /десет/ дни преди изтичане на срока на действието на удостоверението за усъвършенстван електронен подпис, действието на удостоверението за усъвършенстван електронен подпис се прекратява автоматично, с изтичане срокът му на валидност.

- прекратяване действието на удостоверение за усъвършенстван електронен подпис преди изтичане срока на валидност

Действието на удостоверението се прекратява при прекратяване на юридическото лице на доставчика на удостоверителни услуги без прехвърляне на дейността на друг доставчик на удостоверителни услуги.

Доставчикът на удостоверителни услуги прекратява действието на удостоверението при смърт или поставяне под запрещение на Титуляра/Автора.

Доставчикът на удостоверителни услуги прекратява действието на удостоверението при установяване, че удостоверението е издадено въз основа на неверни данни.

Действието на удостоверението предсрочно се прекратява при изразено желание от страна на Титуляра/Автора, заявено лично или по пощата. Необходимо е представяне на заявка за прекратяване на удостоверение (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 Регистрацията орган, се изисква нотариална заверка.

След като се увери в самоличността и извърши допълнителна проверка за достоверност на подадената информация, Регистрацията орган въвежда електронна заявка за промяна в статуса на удостоверението на потребителя. Удостоверяващият орган реализира прекратяването като включва удостоверението за универсален електронен подпис в CRL.