



InfoNotary

ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА УНИВЕРСАЛЕН ЕЛЕКТРОНЕН ПОДПИС ПРЕДОСТАВЯНИ ОТ ИНФОНОТАРИ ЕАД

*Извадка от Наръчник за потребителя
на удостоверителни услуги за универсален електронен подпис*

Версия 1.0

ИНФОНОТАРИ ЕАД

Адрес на управление: ул. "Иван Вазов" № 16, ет.6, 1000 София, България
Съдебна регистрация: № 7719/2004 в Софийски градски съд,
Данъчен №1220187884, БУЛСТАТ 131276827

I. ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА УНИВЕРСАЛЕН ЕЛЕКТРОНЕН ПОДПИС

(1) “Политиката за предоставяне на удостоверявателни услуги за универсален електронен подпис” е документ, неделима част от Наръчника за потребителя, описващ политиката и процедурите, които Доставчикът следва при издаване на удостоверения, както и приложимостта на издаваните удостоверения с оглед сигурността на тези процедури.

(2) За всички типове удостоверения, които издава, Доставчикът разработва и съблюдава различна удостоверявателна политика.

(3) Удостоверявателната политика за тип удостоверение включва правилата, по които се извършват първоначалната идентификация и автентификация на Титулярите и Авторите на удостоверения за електронен подпис, както и политиката за управление на издадените удостоверения – спиране, възобновяване и прекратяване действието на издадено от Доставчика удостоверение.

(4) Удостоверявателната политика на всеки тип удостоверение определя и ограниченията в приложимостта на удостоверенията в зависимост от нивото на сигурност при проверките и степента на доверие в удостоверенията в издадения документ факти.

(5) Удостоверявателните политики на удостоверенията за универсален електронен подпис съдържат и условията и реда за използване на универсалния електронен подпис и изискванията за съхраняване на частния ключ.

I.1. Политика за издаване и управление на Удостоверение за универсален електронен подпис на Физическо лице

I.1.1. Обща характеристика на удостоверението

(1) Удостоверението i-Notary Personal Q Sign има характер на удостоверение за универсален електронен подпис по смисъла на чл. 24 от



ЗЕДЕП и всеки електронен подпис, който е придружен от това удостоверение, има характера на универсален подпис.

(2) Удостоверение за универсален електронен подпис на Физическо лице (i-Notary Personal Q Sign) се издава на физическо лице – Титуляр и Автор, и удостоверява идентичността и връзката с публичния му ключ.

(3) Удостоверението i-Notary Personal Q Sign се издава задължително с генерирани и съхранявани в криптографско устройство (смарт карта) двойка криптографски ключове – частен и публичен, ползвани за създаване и проверка на универсален електронен подпис.

(4) За издаване на удостоверението i-Notary Personal Q Sign се прилагат процедури, осигуряващи високо ниво на надеждност и сигурност на удостоверената информация, идентифицираща Титуляря и Автора и държането на средствата за създаване на електронен подпис – частния ключ.

(5) При процедурите за идентификация и установяване на самоличността на Титуляря и на Автора се изисква представяне на доказателства за самоличността на Титуляря, самоличността на Автора, както и за представителната власт на Автора и личното им явяване пред Регистриращ орган на Доставчика.

1.1.2. Предназначение и приложимост на удостоверението

(1) Удостоверението i-Notary Personal Q Sign може да бъде ползвано като средство за персонална електронна идентификация при електронна търговия, финансови транзакции, електронна кореспонденция, електронно подписване на документи, извършване на изявления от и до държавни органи и органи на местното самоуправление по смисъла на ЗЕДЕП.

(2) В дължимата грижа на Доверяващата се страна е да провери предназначението и приложимостта на това удостоверение, когато се доверява на електронния подпис, който удостоверението придружава.

(3) За проверката от Доверяващата се страна в удостоверението се обозначават политиката, приложима към това удостоверение (“Certificate Policy”), и допълнителните разширения към нея и предназначението и ограниченията на действието на удостоверението, описани в Атрибутите “Key Usage”, “Extended Key Usage”, “Qualified Statements”.

I.1.3. Обозначение

(1) Политиката, приложима към това удостоверение, се обозначава по следния начин:

	Вид политика	Наименование	Обозначение (OID)
	Удостоверителна политика за Удостоверение за универсален електронен подпис на физическо лице	i-Notary Personal Q Sign Certificate CP	1.3.6.1.4.1.22144.1.1.1.1

(2) Политиката е публикувана в Публичния документен регистър на Доставчика и е достъпна на адрес: http://repository.infonotary.com/certpolicy_qsign_personal.html

I.1.4. Профил на удостоверението Personal Q Sign Certificate

Основни x509 атрибути:

Атрибут	Стойност
Версия	3 (0x02)
Сериен номер	Уникален в регистъра на Доставчика; 8-байтово число
Начало на периода на валидност	Датата и часът на подписване на УЕП
Край на периода на валидност	Датата и часът на подписване На УЕП + 1 г.
Алгоритъм на електронния подпис върху УЕП	FIPS DSS; dsaWithSHA1 (1.3.14.3.2.27) или RSA – 2048 бита

Атрибути на издателя (x509 Issuer DN)

Атрибутите на издателя съвпадат с атрибутите на Титуляря на подписващото удостоверение за електронен подпис (УЕП).

Атрибути на Титуляря/Автора (x509 Subject DN):

Атрибут	OID	М ¹	Т/А ²	Стойност
/commonName	2.5.4.3	+	A	
/countryName	2.5.4.6	+	A	
/postalCode	2.5.4.17		T	
/localityName	2.5.4.7		T	
/unstructuredAddress	2.5.4.9	+	T	
/organizationName	2.5.4.10	+	T	
/organizationalUnitName	2.5.4.11			-
/emailAddress	1.2.840.113549.1.9.1		A	
/telephoneNumber	2.5.4.20		T	
Допълнително дефинирани атрибути на организация				
/bgBulstatNumber	2.5.4.10.100.1.2			-
/bgTaxationNumber	2.5.4.10.100.1.1			-
/bgBankAddressableUnit	2.5.4.11.100.1.2			-
/bgBudgetIdentificationNumber	2.5.4.11.100.1.1			-
/bgLegalRegistration	2.5.4.10.100.1.3			-
Допълнително дефинирани атрибути на физическо лице				
/bgUnifiedCitizenNumber	2.5.4.3.100.1.1	+	T	
/bgIdentificationCardNumber	2.5.4.3.100.1.2		T	
/bgFinancialObligationsStatement	2.5.4.3.100.1.3		T	
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4			-

¹ Задължителен (Mandatory)

² Титуляр/Автор

Атрибути на Автора (x509v3 subjectAltName extension DN):

Атрибут	OID	М	Т/А	Стойност
/commonName	2.5.4.3			-
/countryName	2.5.4.6	+	A	
/postalCode	2.5.4.17		A	
/localityName	2.5.4.7		A	
/unstructuredAddress	2.5.4.9		A	
/organizationName	2.5.4.10			-
/organizationalUnitName	2.5.4.11			-
/emailAddress	1.2.840.113549.1.9.1			-
/telephoneNumber	2.5.4.20		A	
Допълнително дефинирани атрибути на организация				
/bgBulstatNumber	2.5.4.10.100.1.2			-
/bgTaxationNumber	2.5.4.10.100.1.1			-
/bgBankAddressableUnit	2.5.4.11.100.1.2			-
/bgBudgetIdentificationNumber	2.5.4.11.100.1.1			-
/bgLegalRegistration	2.5.4.10.100.1.3			-
Допълнително дефинирани атрибути на физическо лице				
/bgUnifiedCitizenNumber	2.5.4.3.100.1.1	+	A	
/bgIdentificationCardNumber	2.5.4.3.100.1.2		A	
/bgFinancialObligationsStatement	2.5.4.3.100.1.3			-
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4	+	A	

Допълнителни x509 атрибути (x509v3 extensions):

Атрибут	OID	М	С ³	Стойност
/basicConstraints	2.5.29.19	+	+	CA=false
/keyUsage	2.5.29.15	+	+	NonRepudiation, DigitalSignature
/extKeyUsage	2.5.29.37	+		emailProtection, clientAuth
/authorityKeyIdentifier	2.5.29.35			subjectKeyIdentifier на подписващото УЕП
/subjectKeyIdentifier	2.5.29.14	+		SHA1 от DER - кодирания публичен ключ
/CRLDistributionPoints	2.5.29.25	+		http://crl.infonotary.com/qsigin-personal-ca.crl ldap://ldap.infonotary.com/dc=qsigin-personal-ca, dc=infonotary, dc=com
/authorityInfoAccess	1.3.6.1.5.5.7.1.1	+		http://ocsp.infonotary.com/responder.cgi
/qcStatements	1.3.6.1.5.5.7.1.3			0.4.0.1862.1.1

CertificatePolicies x509v3 extension:

Идентификатор (OID)	1.3.6.1.4.1.22144.0
CPS	http://www.crc.bg
Текст	Registration Resolution №by the Communication Regulation Commission

Идентификатор (OID)	1.3.6.1.4.1.22144.1.1.1.1
CPS	http://repository.infonotary.com/certpolicy_qsigin_personal.html
Текст	InfoNotary personal qualified certificate

Идентификатор (OID)	0.4.0.1456.1.1
CPS	http://www.infonotary.com/qcp-sscd.html
Текст	This certificate is issued as qualified certificate for advanced electronic signature using secure storage cryptographic device

³ Критично (Critical)

Описание и приложение на атрибутивните OID, използвани в RDN на Удостоверението

Описание на атрибутите

Атрибут	OID	p ⁴	Значение
/commonName	2.5.4.3		Име на субекта
/countryName	2.5.4.6		Код на държавата
/postalCode	2.5.4.17		Пощенски код
/localityName	2.5.4.7		Град/Област
/unstructuredAddress	2.5.4.9		Адрес
/organizationName	2.5.4.10		Име на организацията
/organizationalUnitName	2.5.4.11		Име на подразделение в рамките на организацията
/emailAddress	1.2.840.113549.1.9.1		e-mail адрес
/telephoneNumber	2.5.4.20		Телефонен номер
/bgBulstatNumber	2.5.4.10.100.1.2	+	БУЛСТАТ
/bgTaxationNumber	2.5.4.10.100.1.1	+	Данъчен номер на организацията
/bgBankAddressableUnit	2.5.4.11.100.1.2	+	Банкова адресируема единица
/bgBudgetIdentificationNumber	2.5.4.11.100.1.1	+	Бюджетен идентификационен номер
/bgLegalRegistration	2.5.4.10.100.1.3	+	Информация за съдебната регистрация на организацията
/bgUnifiedCitizenNumber	2.5.4.3.100.1.1	+	Единен граждански номер
/bgIdentificationCardNumber	2.5.4.3.100.1.2	+	Номер на българска лична карта
/bgFinancialObligationsStatement	2.5.4.3.100.1.3	+	Финансови ограничения на документите, подписвани с УЕП
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4	+	Информация за номера и издателя на документа за представителство

Описание на формата и формирането на атрибутите

⁴Собствен (Дефиниран от Доставчика като разширение на съществуващ X.500 атрибут)



Атрибут	Формат	S ⁵	Pr ⁶	Източник
/commonName	A+	,		Трите имена на Автора
/countryName	A2			Двусимволен код на държава
/postalCode	N4			Пощенски код на Титуляря/Автора
/localityName	AN+			Град на Титуляря/Автора
/unstructuredAddress	AN+	,		Данните от адреса на Титуляря/Автора
/organizationName	AN+			Име на организацията на Титуляря/Трите имена на Титуляря, в случай че е физическо лице
/organizationalUnitName	AN+			Име на подразделение в рамките на организацията
/emailAddress	IA5+			e-mail адрес на Автора
/telephoneNumber	AN+			Телефонен номер на Титуляря/Автора
/bgBulstatNumber	N+		BULSTAT:	БУЛСТАТ номер
/bgTaxationNumber	N+		TAXNUMBER:	Данъчен номер
/bgBankAddressableUnit	N+		BAU:	Банкова адресируема единица
/bgBudgetIdentificationNumber	N+		BIN:	Бюджетен идентификационен номер
/bgLegalRegistration	AN+	,	LEGAL:	Информация за съдебната регистрация на организация
/bgUnifiedCitizenNumber	N+		UCN:	Единен граждански номер на Титуляря/Автора
/bgIdentificationCardNumber	N+		IDCARD:	Номер на личната карта на Титуляря/Автора
/bgFinancialObligationsStatement	AN+	:	FO:	Минимална стойност, максимална стойност и ISO код на валута на ограничението
/bgRepresentativeDocumentNumber	AN+		REPDN:	Информация за номера и издателя на документа за представителство

⁵Разделител

⁶Префикс

Колоната “Формат” има следното значение:

Формат	Значение
A	Атрибутът може да приема само буквени стойности
N	Атрибутът може да приема само цифрови стойности
AN	Атрибутът може да приема буквено-цифрени стойности
IA5	Атрибутът може да приема валидни IA5 символи (e-mail/url)

- Числото след обозначението на формата обозначава максимален брой допустими символи.
- Символът ” + “ обозначава един или повече символа.
- Всяко поле, освен маркираните като IA5, съдържа данни в UTF-8 кодиране.
- Датите в полетата за валидност са представени като ASN1 GeneralTime.

I.1.5. Процедура по заявяване издаването на удостоверението

(1) Регистриращите органи на Доставчика приемат и обслужват всички искания за издаване на удостоверения за универсален електронен подпис от крайни потребители.

(2) Искане за издаване на удостоверение до Доставчика могат да отправят всички лица, които:

- ▶ попълнят Искане за издаване на удостоверение;
- ▶ генерират двойка криптографски ключове, самостоятелно или посредством Доставчика;
- ▶ предоставят на Удостоверяващия орган на Доставчика публичния ключ, кореспондиращ на частния ключ;
- ▶ приемат условията на Договора за предоставяне на удостоверителни услуги и Наръчника за потребителя на Доставчика.



(3) Искането за издаване на удостоверение е необходимо да съдържа следните данни:

- информация, индивидуализираща Титуляря, и ако Авторът е различен от Титуляря, и информация за Автора;
- публичния ключ, кореспондиращ на частния ключ от двойката криптографски ключове, генерирани от Титуляря;
- типа на избраното удостоверение.

(4) Искането за издаване на удостоверение е електронен документ във формат PKCS #10, подписан с частния ключ, кореспондиращ на публичния, включен в документа.

(5) Искането за издаване на удостоверение може да бъде създадено през интернет портала на Доставчика и отправено към него посредством криптиран комуникационен канал на адрес: <https://www.infonotary.com>.

(6) Регистриращите органи на Доставчика предоставят услуга на всички лица по генериране на двойката криптографски ключове, създаване на искане за издаване на удостоверение и представянето им пред Доставчика.

(7) Когато Регистриращият орган на Доставчика извършва по искане от Титуляря генериране на двойка криптографски ключове, ползва защитен механизъм за създаването им и ги предоставя на Автора, записани на криптографско защитено устройство – смарт карта или др.

(8) Правата за достъп до частния ключ – ПИН код или парола, се предоставят от Регистриращия орган на Автора в защитен вид.

(9) След предаването от Регистриращия орган на устройството, на което е записан частният ключ и правата за достъп до него, Титулярят и Авторът носят пълната отговорност за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на техния частен ключ.

I.1.6. Потвърждаване или отхвърляне на заявките за удостоверения

(1) За установяване и потвърждаване на самоличността на физическо лице, направено искане за издаване на удостоверение, се прилагат процедури и спазват правила, определени от Доставчика.

(2) Проверките и потвърждаването на информацията се извършват от Регистриращия орган съобразно правилата и процедурите на Доставчика и в пълно съответствие с Наръчника за потребителя и други вътрешни документи.

(3) Регистриращият орган проверява и потвърждава следната информация, идентифицираща Физическото лице – Титуляр, Автор или упълномощен представител на Титуляря:

- лично, бащино и фамилно име;
- дата на раждане;
- място на раждане;
- националност;
- пол;
- адрес, град, държава, пощенски код;
- Единен граждански номер (ЕГН);
- номер на документ за самоличност: лична карта, паспорт;
- издател, дата на издаване и валидност на документа за самоличност;
- представителната власт на Автора и/или Представителя;
- информация за контакти и фактуриране.

(4) Титулярят, Авторът или упълномощения представител на Титуляря представят лично пред Регистриращия орган следните документи:

- валиден документ за самоличност: лична карта или паспорт;
- нотариално заверено пълномощно за упълномощаване на Представителя да представлява Титуляря пред Доставчика за



издаване и управление на удостоверения;

- документ, доказващ представителната власт на Автора – съдебно решение, удостоверение за актуално състояние, нотариално заверено пълномощно или друг овластяващ акт.

(5) Преди потвърждаване на подадено искане за издаване на удостоверение Регистриращият орган на Доставчика извършва необходимите проверки, като:

- ▶ проверява и потвърждава самоличността или идентичността на Заявителя, Автора, Титуляря или представляващото го лице по предоставените от тях документи;
- ▶ проверява и потвърждава представителната власт на Автора и упълномощеното от Титуляря да го представлява лице;
- ▶ проверява коректността на получената или направената подписана електронна заявка (във формат PKCS#10) за издаване на удостоверение;
- ▶ предоставя на Титуляря или Автора информацията, която е потвърдена и ще бъде включена в издаденото удостоверение за приемане на съдържанието му.

(6) След направените проверки и приемане на съдържанието на удостоверението от Титуляря или Автора Регистриращият орган потвърждава искането за издаване на удостоверение към Удостоверяващия орган на Доставчика и гарантира, че:

- искането за издаване изхожда от Титуляря или от надлежно овластено от него лице или от Автора;
- информацията относно Титуляря и Автора, представена за включване в удостоверението, е вярна и пълна;
- частният ключ е технически годен да бъде използван за създаване на усъвършенстван електронен подпис и съответства на публичния ключ, така че чрез публичния ключ може да се удостовери, че определен електронен подпис е създаден с частния ключ, и

- частният ключ се държи от Автора.

(7) Ако процесът на потвърждаване на заявката за издаване на удостоверение завърши неуспешно, Регистриращият орган отхвърля искането за издаване на удостоверение.

(8) Регистриращият орган незабавно уведомява Заявителя и посочва причината за отхвърлянето директно или посредством:

- ▶ изпращане на електронно писмо до Титуляря, респективно Автора и
- ▶ публикуване на информация за издаването в интернет портала на Доставчика, когато Титулярят или Авторът са регистрирани потребители и притежават валидни права за достъп до портала на адрес: <http://www.infonotary.com>.

(9) Заявители, чиито искания за издаване на удостоверение са били отхвърлени, могат отново да подадат искане за издаване на удостоверение.

(10) Регистриращият орган окомплектова и съхранява предоставените от Титуляря, Автора и Заявителя документи заедно с искането за издаване на удостоверение и подписан договор за удостоверяващи услуги.

(11) Доставчикът контролира точността на включената в удостоверението информация, предоставена на Титуляря и Автора към момента на издаване на удостоверението.

(12) Проверката и потвърждаването на информацията в направените искания за издаване на удостоверения се обработват в разумен срок и Доставчикът издава удостоверенията до 5 работни дни от датата на приемане на документите.

I.1.7. Издаване на Удостоверението

(1) Удостоверяващия орган на Доставчика издава удостоверението на база на получено искане за издаване от Регистриращия орган.



(2) Искането за издаване на удостоверение от Регистриращия орган гарантира потвърждаването на валидността на заявката, направена от Заявителя, валидността на данните, съдържащи се в нея, и е подписано от администратора на Регистриращия орган, извършил проверките.

(3) Удостоверяващия орган на Доставчика проверява идентичността на Регистриращия орган и самоличността на администратора на Регистриращия орган на база на представени пълномощия (специално административно удостоверение на администратор на Регистриращ орган).

(4) След издаване на удостоверението Доставчикът го доставя до Титуляря, съответно до Автора:

- ▶ чрез публикуване на връзка за дънлоуд на удостоверението в интернет портала на Доставчика, когато Титулярят или Авторът са регистрирани потребители и притежават валидни права за достъп до портала на адрес: <http://www.infonotary.com>
- ▶ или посредством Регистриращия орган.

I.1.8. Приемане на удостоверението

(1) Доставчикът издава удостоверението в съответствие със съгласието на Титуляря, респ. Автора.

(2) Приемане на съдържанието на удостоверението се удостоверява с подписване на Протокол за приемане на удостоверение за универсален електронен подпис от Титуляря, респ. Автора преди публикуването му в Регистъра на удостоверенията на Доставчика.

I.1.9. Публикуване на удостоверението от Удостоверяващия орган

Доставчикът публикува незабавно издаденото удостоверение за универсален електронен подпис в Регистъра на удостоверенията си.

I.1.10. Спиране и възобновяване на удостоверението

Спирането и възобновяването на удостоверението се извършва по общите процедури за Спиране на удостоверения и Възобновяване на удостоверения съгласно т. 4.9.11 и т. 4.9.16 от Наръчника за потребителя.

I.1.11. Прекратяване на удостоверението

Прекратяването на удостоверението се извършва по общите процедури за Прекратяване на удостоверения съгласно т. 4.9 от Наръчника за потребителя.

I.1.12. Подновяване на удостоверението

Подновяване на удостоверението се извършва по общите процедури за Прекратяване на удостоверения съгласно т. 4.6 от Наръчника за потребителя.

I.2. Политика за издаване и управление на Удостоверение за универсален електронен подпис на Юридическо лице

I.2.1. Обща характеристика на удостоверението

(1) Удостоверението i-Notary Company Q Sign има характер на удостоверение за универсален електронен подпис по смисъла на чл. 24 от ЗЕДЕП и всеки електронен подпис, който е придружен от това удостоверение, има характера на универсален подпис.

(2) Удостоверение за универсален електронен подпис на Юридическо лице (i-Notary Company Q Sign) се издава на юридическо лице – Титуляр, и удостоверява идентичността и връзката с публичния му ключ.

(3) Удостоверението i-Notary Company Q Sign се издава задължително с генерирани и съхранявани в криптографско устройство (смарт карта) на двойката криптографски ключове – частен и публичен, ползвани за създаване и проверка на универсален електронен подпис.

(4) За издаване на удостоверението i-Notary Company Q Sign се прилагат процедури, осигуряващи високо ниво на надеждност и сигурност на удостоверената информация, идентифицираща Титуляря и Автора и

държането на средствата за създаване на електронен подпис – частния ключ.

(5) При процедурите за идентификация и установяване на самоличността на Титуляря и на Автора се изисква представяне на доказателства за самоличността на Титуляря, самоличността на Автора, както и за представителната власт на Автора и личното им явяване пред Регистриращ орган на Доставчика.

I.2.2. Обозначение

(1) Политиката, приложима към това удостоверение, се обозначава по следния начин:

Вид политика	Наименование	Обозначение (OID)
Удостоверителна политика за Удостоверение за универсален електронен подпис на Юридическо лице	i-Notary Company Q Sign Certificate CP	1.3.6.1.4.1.22144.1.1.2.1

(2) Политиката е публикувана в Публичния документен регистър на Доставчика и е достъпна на адрес:

http://repository.infonotary.com/certpolicy_qsign-company.html.

I.2.3. Предназначение и приложимост на удостоверението

(1) Удостоверение за универсален електронен подпис на Юридическо лице (i-Notary Company Q Sign certificate) може да бъде ползвано като средство за фирмена/професионална електронна идентификация, електронна търговия, финансови транзакции, електронна кореспонденция, електронно подписване на документи, извършване на изявления от и до държавни органи и органи на местното самоуправление по смисъла на ЗЕДЕП.



(2) В дължимата грижа на Доверяващата се страна е да провери предназначението и приложимостта на това удостоверение, когато се доверява на електронния подпис, който удостоверението придружава.

(3) За проверката от Доверяващата се страна в удостоверението се обозначават политиката, приложима към това удостоверение ("Certificate Policy"), и допълнителните разширения към нея и предназначението и ограниченията на действието на удостоверението, описани в Атрибутите "Key Usage", "Extended Key Usage", "Qualified Statements".

I.2.4. Профил на удостоверението Company Q Sign Certificate

I.2.5. Основни Атрибути (x509)

Атрибут	Стойност
Версия	3 (0x02)
Сериен номер	Уникален в регистъра на Доставчика; 8-байтово число
Начало на периода на валидност	Датата и часът на подписване на УЕП
Край на периода на валидност	Датата и часът на подписване на УЕП+ 1 г.
Алгоритъм на електронния подпис върху УЕП	FIPS DSS; dsaWithSHA1 (1.3.14.3.2.27) или RSA – 2048 бита

Атрибути на издателя (x509 Issuer DN)

Атрибутите на издателя съвпадат с атрибутите на Титуляря на подписващото удостоверение за електронен подпис (УЕП).

Атрибути на Титуляря/Автора (x509 Subject DN):

Атрибут	OID	М ⁷	Т/А ⁸	Стойност
/commonName	2.5.4.3	+	A	
/countryName	2.5.4.6	+	A	
/postalCode	2.5.4.17		T	
/localityName	2.5.4.7		T	
/unstructuredAddress	2.5.4.9	+	T	
/organizationName	2.5.4.10	+	T	
/organizationalUnitName	2.5.4.11			-
/emailAddress	1.2.840.113549.1.9.1		A	
/telephoneNumber	2.5.4.20		T	
Допълнително дефинирани атрибути на организация				
/bgBulstatNumber	2.5.4.10.100.1.2			-
/bgTaxationNumber	2.5.4.10.100.1.1			-
/bgBankAddressableUnit	2.5.4.11.100.1.2			-
/bgBudgetIdentificationNumber	2.5.4.11.100.1.1			-
/bgLegalRegistration	2.5.4.10.100.1.3			-
Допълнително дефинирани атрибути на физическо лице				
/bgUnifiedCitizenNumber	2.5.4.3.100.1.1	+	T	
/bgIdentificationCardNumber	2.5.4.3.100.1.2		T	
/bgFinancialObligationsStatement	2.5.4.3.100.1.3		T	
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4			-

⁷ Задължителен (Mandatory)

⁸ Титуляр/Автор

Атрибути на Автора (x509v3 subjectAltName extension DN):

Атрибут	OID	М	Т/А	Стойност
/commonName	2.5.4.3			-
/countryName	2.5.4.6	+	A	
/postalCode	2.5.4.17		A	
/localityName	2.5.4.7		A	
/unstructuredAddress	2.5.4.9		A	
/organizationName	2.5.4.10			-
/organizationalUnitName	2.5.4.11			-
/emailAddress	1.2.840.113549.1.9.1			-
/telephoneNumber	2.5.4.20		A	
Допълнително дефинирани атрибути на организация				
/bgBulstatNumber	2.5.4.10.100.1.2			-
/bgTaxationNumber	2.5.4.10.100.1.1			-
/bgBankAddressableUnit	2.5.4.11.100.1.2			-
/bgBudgetIdentificationNumber	2.5.4.11.100.1.1			-
/bgLegalRegistration	2.5.4.10.100.1.3			-
Допълнително дефинирани атрибути на физическо лице				
/bgUnifiedCitizenNumber	2.5.4.3.100.1.1	+	A	
/bgIdentificationCardNumber	2.5.4.3.100.1.2		A	
/bgFinancialObligationsStatement	2.5.4.3.100.1.3			-
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4	+	A	

Допълнителни x509 атрибути (x509v3 extensions):

Атрибут	OID	М	С ⁹	Стойност
/basicConstraints	2.5.29.19	+	+	CA=false
/keyUsage	2.5.29.15	+	+	NonRepudiation,DigitalSignature
/extKeyUsage	2.5.29.37	+		emailProtection, clientAuth
/authorityKeyIdentifier	2.5.29.35			subjectKeyIdentifier на подписващото УЕП.
/subjectKeyIdentifier	2.5.29.14	+		SHA1 от DER-кодирания публичен ключ
/CRLDistributionPoints	2.5.29.25	+		http://crl.infonotary.com/crl/ qsign-corporate-ca.crl ldap://ldap.infonotary.com/dc=qsign-corporate-ca, dc=infonotary,dc=com
/authorityInfoAccess	1.3.6.1.5.5.7.1.1	+		http://ocsp.infonotary.com/responder.cgi
/qcStatements	1.3.6.1.5.5.7.1.3			0.4.0.1862.1.1

CertificatePolicies x509v3 extension:

Идентификатор (OID)	1.3.6.1.4.1.22144.0
CPS	http://www.crc.bg
Текст	Registration Resolution №by the Communication Regulation Commission

Идентификатор (OID)	1.3.6.1.4.1.22144.1.1.2.1
CPS	http://repository.infonotary.com/certpolicy_qsign-company.html
Текст	This certificate is issued to the subject in order to legally represent the organization as stated above

Идентификатор (OID)	0.4.0.1456.1.1
CPS	http://www.infonotary.com/qcp-sscd.html
Текст	This certificate is issued as qualified certificate for advanced electronic signature using secure storage cryptographic device

⁹ Критично (Critical)

Описание и приложение на атрибутивните OID, използвани в RDN на Удостоверението

Описание на атрибутите

Атрибут	OID	p ¹⁰	Значение
/commonName	2.5.4.3		Име на субекта
/countryName	2.5.4.6		Код на държавата
/postalCode	2.5.4.17		Пощенски код
/localityName	2.5.4.7		Град/Област
/unstructuredAddress	2.5.4.9		Адрес
/organizationName	2.5.4.10		Име на организацията
/organizationalUnitName	2.5.4.11		Име на подразделение в рамките на организацията
/emailAddress	1.2.840.113549.1.9.1		e-mail адрес
/telephoneNumber	2.5.4.20		Телефонен номер
/bgBulstatNumber	2.5.4.10.100.1.2	+	БУЛСТАТ
/bgTaxationNumber	2.5.4.10.100.1.1	+	Данъчен номер на организацията
/bgBankAddressableUnit	2.5.4.11.100.1.2	+	Банкова адресируема единица
/bgBudgetIdentificationNumber	2.5.4.11.100.1.1	+	Бюджетен идентификационен номер
/bgLegalRegistration	2.5.4.10.100.1.3	+	Информация за съдебната регистрация на организацията
/bgUnifiedCitizenNumber	2.5.4.3.100.1.1	+	Единен граждански номер
/bgIdentificationCardNumber	2.5.4.3.100.1.2	+	Номер на българска лична карта
/bgFinancialObligationsStatement	2.5.4.3.100.1.3	+	Финансови ограничения на документите, подписвани с УЕП
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4	+	Информация за номера и издателя на документа за представителство

Описание на формата и формирането на атрибутите

¹⁰ Собствен (Дефиниран от Доставчика като разширение на съществуващ X.500 атрибут)

Атрибут	Формат	S ¹¹	Pr ¹²	Източник
/commonName	A+	,		Трите имена на Автора
/countryName	A2			Двусимволен код на държава
/postalCode	N4			Пощенски код на Титуляря/Автора
/localityName	AN+			Град на Титуляря/Автора
/unstructuredAddress	AN+	,		Данните от адреса на Титуляря/Автора
/organizationName	AN+			Име на организацията на Титуляря / Трите имена на Титуляря, в случай че е физическо лице
/organizationalUnitName	AN+			Име на подразделение в рамките на организацията
/emailAddress	IA5+			e-mail адрес на Автора
/telephoneNumber	AN+			Телефонен номер на Титуляря/Автора
/bgBulstatNumber	N+		BULSTAT:	БУЛСТАТ номер
/bgTaxationNumber	N+		TAXNUM:	Данъчен номер
/bgBankAddressableUnit	N+		BAU:	Банкова адресируема единица
/bgBudgetIdentificationNumber	N+		BIN:	Бюджетен идентификационен номер
/bgLegalRegistration	AN+	,	LEGAL:	Информация за съдебната регистрация на организация
/bgUnifiedCitizenNumber	N+		UCN:	Единен граждански номер на Титуляря/Автора
/bgIdentificationCardNumber	N+		IDCARD:	Номер на личната карта на Титуляря/Автора
/bgFinancialObligationsStatement	AN+	:	FO:	Минимална стойност, максимална стойност и ISO код на валута на ограничението
/bgRepresentativeDocumentNumber	AN+		REPDN:	Информация за номера и издателя на документа за представителство

¹¹Разделител

¹²Префикс



Колоната “Формат” има следното значение:

Формат	Значение
A	Атрибутът може да приема само буквени стойности
N	Атрибутът може да приема само цифрови стойности
AN	Атрибутът може да приема буквено-цифрени стойности
IA5	Атрибутът може да приема валидни IA5 символи (e-mail/url)

- Числото след обозначението на формата обозначава максимален брой допустими символи.*
- Символът ” + “ обозначава един или повече символа.*
- Всяко поле, освен маркираните като IA5, съдържа данни в UTF-8 кодиране.*
- Датите в полетата за валидност са представени като ASN1 GeneralTime.*

I.2.6. Процедура по заявяване издаването на удостоверение

(1) Регистриращите органи на Доставчика приемат и обслужват всички искания за издаване на удостоверения за универсален електронен подпис от крайни потребители.

(2) Искане за издаване на удостоверение до Доставчика могат да отправят всички лица, които:

- ▶ попълнят Искане за издаване на удостоверение;
- ▶ генерират двойка криптографски ключове, самостоятелно или посредством Доставчика;
- ▶ предоставят на Удостоверяващия орган на Доставчика публичния ключ, кореспондиращ на частния ключ;



- ▶ приемат условията на Договора за предоставяне на удостоверявателни услуги и Наръчника за потребителя на Доставчика.

(3) Искането за издаване на удостоверение е необходимо да съдържа следните данни:

- информация, индивидуализираща Титуляря, и ако Авторът е различен от Титуляря, и информация за Автора;
- публичния ключ, кореспондиращ на частния ключ от двойката криптографски ключове, генерирани от Титуляря;
- типа на избраното удостоверение.

(4) Искането за издаване на удостоверение е електронен документ във формат PKCS #10, подписан с частния ключ, кореспондиращ на публичния, включен в документа.

(5) Искането за издаване на удостоверение може да бъде създадено през интернет портала на Доставчика и отправено към него посредством криптиран комуникационен канал на адрес: <https://www.infonotary.com>.

(6) Регистриращите органи на Доставчика предоставят услуга на всички лица по генериране на двойката криптографски ключове, създаване на искане за издаване на удостоверение и представянето им пред Доставчика.

(7) Когато Регистриращият орган на Доставчика извършва по искане от Титуляря генериране на двойка криптографски ключове, ползва защитен механизъм за създаването им и ги предоставя на Автора, записани на криптографско защитено устройство – смарт карта или др.

(8) Правата за достъп до частния ключ – ПИН код или парола, се предоставят от Регистриращия орган на Автора в защитен вид.

(9) След предаването от Регистриращия орган на устройството, на което е записан частният ключ и правата за достъп до него, Титулярят и Авторът носят пълната отговорност за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на техния частен ключ.

I.2.7. Потвърждаване или отхвърляне на заявките за удостоверения

(1) За установяване и потвърждаване на идентичността на юридическо лице, направено искане за издаване на удостоверение, се прилагат процедури и спазват правила, определени от Доставчика в Наръчника за потребителя.

(2) Доставчикът си запазва правото да променя изискванията към информацията и документите, необходими за потвърждаване на идентификацията на Титуляря – Юридическо лице, при необходимост от изпълнение на свои удостоверителни политики или изисквания на закона.

(3) Проверките и потвърждаването на информацията се извършват от Регистриращия орган съобразно правилата и процедурите на Доставчика и в пълно съответствие с Наръчника за потребителя и други вътрешни документи.

(4) Регистриращият орган проверява и потвърждава следната информация, идентифицираща Юридическо лице - Титуляр:

- наименование на юридическото лице;
- адрес, град, държава, пощенски код;
- номер по национален данъчен регистър и/или
- номер по БУЛСТАТ;
- име на домейн;
- правен статут и актуално състояние;
- право върху търговско име, марка, домейн и др.;
- информация за контакт и фактуриране.

(5) Титулярят, респективно упълномощен представител на Титуляря представя лично пред Регистриращия орган следните документи:

- съдебно решение за регистрация или акт за възникване;
- удостоверение за актуално състояние, издадено не по-рано от 1 месец от датата на представяне;
- документ за регистрация по БУЛСТАТ;
- документ за данъчна регистрация;



- документ за доказване на право за ползване на име и др.

(4) Титулярят, Авторът или упълномощеният представител на Титуляря представят лично пред Регистриращия орган следните документи:

- валиден документ за самоличност: лична карта или паспорт;
- нотариално заверено пълномощно за упълномощаване на Представителя да представлява Титуляря пред Доставчика за издаване и управление на удостоверения;
- документ, доказващ представителната власт на Автора – съдебно решение, удостоверение за актуално състояние, нотариално заверено пълномощно или друг овластяващ акт.

(5) Преди потвърждаване на подадено искане за издаване на удостоверение Регистриращият орган на Доставчика извършва необходимите проверки, като:

- ▶ проверява и потвърждава самоличността или идентичността на Заявителя, Автора, Титуляря или представляващото го лице по предоставените от тях документи;
- ▶ проверява и потвърждава представителната власт на Автора и упълномощеното от Титуляря да го представлява лице;
- ▶ проверява коректността на получената или направената подписана електронна заявка (във формат PKCS#10) за издаване на удостоверение;

предоставя на Титуляря или Автора информацията, която е потвърдена и ще бъде включена в издаденото удостоверение за приемане на съдържанието му.

(6) След направените проверки и приемане на съдържанието на удостоверението от Титуляря или Автора Регистриращият орган потвърждава искането за издаване на удостоверение към Удостоверяващия орган на Доставчика и гарантира че:



- искането за издаване изхожда от Титуляря или от надлежно овластено от него лице или от Автора;
- информацията относно Титуляря и Автора, представена за включване в удостоверението, е вярна и пълна;
- частният ключ е технически годен да бъде използван за създаване на усъвършенстван електронен подпис и съответства на публичния ключ, така че чрез публичния ключ може да се удостовери, че определен електронен подпис е създаден с частния ключ и
- частният ключ се държи от Титуляря или съответно от Автора.

(7) Ако процесът на потвърждаване на заявката за издаване на удостоверение завърши неуспешно, Регистриращият орган отхвърля искането за издаване на удостоверение.

(8) Регистриращият орган незабавно уведомява Заявителя и посочва причината за отхвърлянето директно или посредством:

изпращане на електронно писмо до Титуляря, респективно Автора и

публикуване на информация за издаването в интернет портала на Доставчика, когато Титулярят или Авторът са регистрирани потребители и притежават валидни права за достъп до портала на адрес: <http://www.infonotary.com>.

(9) Заявители, чиито искания за издаване на удостоверение са били отхвърлени, могат отново да подадат искане за издаване на удостоверение.

(10) Регистриращият орган окомплектова и съхранява предоставените от Титуляря, Автора и Заявителя документи заедно с искането за издаване на удостоверение и подписан договор за удостоверявателни услуги.

(11) Доставчикът контролира точността на включената в удостоверението информация, предоставена на Титуляря и Автора към момента на издаване на удостоверението.

(12) Проверката и потвърждаването на информацията в направените искания за издаване на удостоверения се обработват в разумен срок и

Доставчикът издава удостоверенията до 5 работни дни от датата на приемане на документите.

I.2.8. Издаване на удостоверението

(1) Удостоверяващия орган на Доставчика издава удостоверението на база на получено искане за издаване от Регистриращия орган.

(2) Искането за издаване на удостоверение от Регистриращия орган гарантира потвърждаването на валидността на заявката, направена от Заявителя, валидността на данните, съдържащи се в нея, и е подписано от администратора на Регистриращия орган, извършил проверките.

(3) Удостоверяващия орган на Доставчика проверява идентичността на Регистриращия орган и самоличността на администратора на Регистриращия орган на база на представени пълномощия (специално административно удостоверение на администратор на Регистриращ орган).

(4) След издаване на удостоверението Доставчикът го доставя до Титуляря, съответно до Автора:

чрез публикуване на връзка за дънлоуд на удостоверението в интернет портала на Доставчика, когато Титулярят или Авторът са регистрирани потребители и притежават валидни права за достъп до портала на адрес: <http://www.infonotary.com>

или посредством Регистриращия орган.

I.2.9. Приемане на удостоверението

(1) Доставчикът издава удостоверението в съответствие със съгласието на Титуляря, респ. Автора.

(2) Приемане на съдържанието на удостоверението се удостоверява с подписване на Протокол за приемане на удостоверение от Титуляря, респ. Автора преди публикуването му в Регистъра на удостоверенията на Доставчика.

I.2.10. Публикуване на удостоверението от Удостоверяващия орган

Доставчикът публикува незабавно издаденото удостоверение в Регистъра на удостоверенията си.

I.2.11. Спиране и възобновяване на удостоверението

Спирането и възобновяването на удостоверението се извършва по общите процедури за Спиране на удостоверения и Възобновяване на удостоверения съгласно т. 4.9.11 и т. 4.9.16 от Наръчника за потребителя.

I.2.12. Прекратяване на удостоверението

Прекратяването на удостоверението се извършва по общите процедури за Прекратяване на удостоверения съгласно т. 4.9 от Наръчника за потребителя.

I.2.13. Подновяване на удостоверението

Подновяване на удостоверението се извършва по общите процедури за Прекратяване на удостоверения съгласно т. 4.6 от Наръчника за потребителя.